Yale Journal of Health Policy, Law, and Ethics

Volume 16 | Issue 1 Article 1

2016

The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work

Elizabeth A. Brown
Assistant Professor of Business Law, Bentley University.

The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work

Elizabeth A. Brown*

Abstract:

Employers are collecting and using their employees' health data, mined from wearable fitness devices and health apps, in new, profitable, and barely regulated ways. The importance of protecting employee health and fitness data will grow exponentially in the future. This is the moment for a robust discussion of how law can better protect employees from the potential misuse of their health data.

While scholars have just begun to examine the problem of health data privacy, this Article contributes to the academic literature in three important ways. First, it analyzes the convergence of three trends resulting in an unprecedented growth of health-related data: the Internet of Things, the Quantified Self movement, and the Rise of Health Platforms. Second, it describes the insufficiencies of specific data privacy laws and federal agency actions in the context of protecting employee health data from employer misuse. Finally, it provides two detailed and workable solutions for remedying the current lack of protection of employee health data that will realign employer use with reasonable expectations of health and fitness privacy.

The Article proceeds in four Parts. Part I describes the growth of self-monitoring apps, devices, and other sensor-enabled technology that can monitor a wide range of data related to an employee's health and fitness and the relationship of this growth to both the Quantified Self movement and the Internet of Things. Part II explains the increasing use of employee monitoring through a wide range of sensors, including wearable devices, and the potential uses of that health and fitness data. Part III explores the various regulations and agency actions that might protect employees from the potential misuse of their health and fitness data and the shortcomings of each. Part IV proposes two specific measures that would help ameliorate the ineffective legal protections that currently exist in this context. In order to improve employee notice of and control over the disclosure of their health data, I recommend the adoption of a mandatory privacy labeling law for health-related devices and apps to be enacted and enforced by the Federal Trade Commission (FTC). As a complementary measure,

* Assistant Professor of Business Law, Bentley University. The author wishes to thank Sharon Patton for her invaluable assistance with this Article.

I also recommend that be amended so that its protections extend to the health-related data that employers may acquire about their employees. The Article concludes with suggestions for additional scholarly discussion.

TABLE OF CONTENTS

INTRODUCTION

Imagine coming to work one day and finding that your employer has given everyone in the company a wearable Fitbit health monitor, free of charge. You pop the Fitbit on, grateful for another bit of help in managing the health concerns that nag at you persistently but which never quite rise to the top of your priority list. At your next performance review, your supervisor expresses concern about your anxiety levels. Although your work output is slightly off, she notes, there has been a correlation in your lack of sleep and exercise, and she suspects you are depressed. You wonder how your employer might know these things, whether or not they are true, and then you remember the Fitbit. Your supervisor then tells you that the promotion you had wanted is going to a colleague who is "better equipped to handle the demands of the job." You interview for another job and are asked to provide access to the Apple Health account that centralizes the fitness data your iPhone apps collect.

Similar scenarios are likely to play out now and more frequently in the future as the personal health sensor market and employee monitoring trends continue to grow. Employers make key decisions based on employees' biometric data, collected from specialized devices like a Fitbit or the health-related apps installed on mobile phones. BP, for example, adjusts its employees' health care premiums depending on how much physical activity their wearable Fitbit devices monitor—devices that BP provides to thousands of employees, their spouses, and retirees for free.[1] These programs are not always optional. Employers are already starting to require their workers to submit health metrics or pay a fine. For example, CVS Pharmacy demands that every one of the 200,000 employees who use its health plan provide certain information about their weight, glucose levels, and body fat.[2] Although CVS calls its plan "voluntary," covered workers who refuse to provide this information must pay a fine of $50 per month.

Gathering employee data from health monitoring devices and apps provides a substantial benefit to employers and poses substantial risks to employees. The benefits include a relatively user-friendly means of improving health and, correspondingly, reducing workplace losses due to illness and absence. Incidence of obesity, adult-onset diabetes, and many other serious health conditions that have a behavioral component are a serious issue in the United States. Health

---

1 Parmy Olson & Aaron Tilley, *The Quantified Other: Nest and Fitbit Chase a Lucrative Side Business*, FORBES (Apr. 17, 2014, 4:30 AM), http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest-and-fitbit-chase-a-lucrative-side-business.

2 Steve Osunsami, *CVS Pharmacy Wants Workers' Health Information, or They'll Pay a Fine*, ABC NEWS (Mar. 20, 2013), http://abcnews.go.com/blogs/health/2013/03/20/cvs-pharmacy-wants-workers-health-information-or-theyll-pay-a-fine.

monitoring devices and apps claim great success in improving weight, BMI, and heart rate.

The risks to employees, however, include the potential for adverse employment decisions, discrimination, and invasions of privacy rights that no federal law currently prohibits. The increasing coalescence of fitness-related data from apps and devices makes it increasingly likely that employers will monitor and act on employee's health data. Each data point is valuable in itself, and even more so in combination. Greater access to both heart rate data and sleep patterns, for example, might give an employer more insight into an employee's overall health than either input alone. Legal scholars have started to ask whether such monitoring is sufficiently limited by existing laws.[3] What limits employers from getting and using these data for various potentially undesirable (if not illegal) purposes?

In this Article, I argue that federal law does not do enough to protect employees' health and fitness data from potential misuse, while employers have every incentive to use these data in hiring, promotion, and related decisions and that two specific remedies would do much to curtail the improper use of employee health and fitness data.

This Article proceeds in four Parts. Part I describes the growth of self-monitoring apps, devices, and other sensor-enabled technology that can monitor a wide range of data related to an employee's health and fitness and the relationship of this growth to both the Quantified Self movement and the Internet of Things.[4] Part II explains the increasing use of employee monitoring through a wide range of sensors, including wearable devices, and the potential uses of that health and fitness data. Part III explores the regulations and agency actions that might protect employees from the potential misuse of their health and fitness data and the shortcomings of each. Part IV proposes two specific measures that would help ameliorate the ineffective legal protections that currently exist. In order to improve employee notice of and control over the disclosure of their health data, I

3 *See, e.g.*, Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY. L.J 345, 345 (2015); Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent*, 93 TEX. L. REV. 85, 93-95 (2014); Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH 6, 7 (2015); N. Nina Zivanovic, *Medical Information as a Hot Commodity: The Need for Stronger Protection of Patient Health Information*, 19 INTELL. PROP. L. BULL. 183, 185 (2015); *see also* Lauren Henry, *Information Privacy and Data Security*, 2015 CARDOZO L. REV. DE NOVO 107, 109 (discussing the complex relationship between the goals of data security and information privacy).

4 The technology described in Part I and throughout the Article can be used by any consumer, but I use the term "employee" because the focus of this Article is on the impact of such technological advances in the employment context.

recommend the adoption of a mandatory privacy labeling law for health-related devices and apps to be enacted and enforced by the Federal Trade Commission (FTC). As a complementary measure, I also recommend that Health Insurance Portability and Accountability Act of 1996 (HIPAA)[5] be amended so that its protections extend to the health-related data that employers may acquire about their employees. The Article concludes with suggestions for additional scholarly discussion.

I. EMPLOYEES GENERATE HEALTH AND FITNESS DATA THROUGH INCREASINGLY UBIQUITOUS SENSORS

The wearable health technology market is growing fast. Every January, technology cognoscenti descend on Las Vegas for the International Consumer Electronics Show (CES), one of the largest electronics shows in the world with over two million square feet of exhibition space.[6] In 2014, the Wearable and Fitness sections took up a few hundred square feet of space at CES. In 2015, the Wearable and Fitness categories together took up almost half of the cavernous exhibition hall.[7]

The mobile health market includes a range of consumer devices equipped with sensors and software-based apps that help monitor and collect health-related data. That market is expected to grow eight-fold in less than ten years, from $5.1 billion in 2013 to $41.8 billion in 2023.[8] The number of wearable fitness devices sold annually is expected nearly to triple between 2014 and 2018.[9]

One of the most popular examples is the Fitbit. Fitbit makes several versions of a wearable device that "tracks every part of your day—including activity, exercise, food, weight and sleep," according to its website.[10]. Its flagship device is a sensor worn on the wrist, like a watch, that records the user's heart rate and movement, among other data. Other Fitbit devices can be clipped to a user's clothes or shoes and perform similar functions. Specifically, Fitbit devices record

---

5 The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

6 *CES by the Numbers*, CONSUMER TECH. ASS'N, http://www.cesweb.org/Why-CES-/CES-By-the-Numbers.aspx (last visited Dec. 1, 2015).

7 Daniel Cooper, *2015 Is the Year that Wearables Begin To Grow up*, ENGADGET (Jan. 10, 2015, 1:13 AM), http://www.engadget.com/2015/01/10/2015-ces-wearables-wrap-up/.

8 Carole Jacques, *Mobile Health Devices Market To Grow 8-Fold to $41.8 Billion in 2023*, LUX RES. (July 1, 2014), http://www.luxresearchinc.com/news-and-events/press-releases/read/mobile-health-devices-market-grow-8-fold-418-billion-2023.

9 Fred Pennic, *Fitness Devices To Dominate the Wearables Market Until 2018*, HIT CONSULTANT (Nov. 25, 2014), http://hitconsultant.net/2014/11/25/fitness-devices-to-dominate-the-wearables-market-until-2018.

10 *Why Fitbit*, FITBIT, https://www.Fitbit.com/whyFitbit (last visited Dec. 1, 2015).

"sleep tracking," "auto sleep detection," continuous heart rate, floors climbed, and "active minutes," although the specific combination of surveillance features depends on the model.[11] Some models also track the user's GPS location.[12] The device works in conjunction with an app that displays these data and which can be accessed from a smartphone or a computer. The data display, or "dashboard," allows the user to track their own activity, set goals, and earn "badges" for meeting specific activity goals.[13] Fitbit dashboard users may monitor their calorie intake by using their smartphones to scan nutrition labels.[14] The dashboard also syncs with the Aria, Fitbit's "wi-fi smart scale," for more comprehensive weight management.[15] Fitbits are available in a range of models, each with different features and recommended retail prices.[16]

Fitbit makes just a few of the thousands of health-monitoring devices, which often work in conjunction with mobile phone apps like the Fitbit dashboard, that record personal health data. These devices are so popular that one in ten Americans over the age of eighteen now owns an activity tracker.[17]

Wearables can measure many other kinds of data that employers might consider relevant in management, such as wellbeing and mood. Zensorium's Being, introduced at CES in 2015, is a watch-like device that indicates whether the wearer's mood is Distress, Excited, Normal, or Calm.[18] It is easy to imagine a supervisor's interest in monitoring employees' moods remotely, especially when those employees are engaged in heavily interpersonal roles like sales or customer service.[19] Other wearable technology promises to influence mood directly. Thync, a company founded by neurobiology, neuroscience and consumer electronics experts from Harvard, MIT, and Stanford, developed a sensor that attaches to the temple and changes the wearer's mental state either to energized

---

11 *Find Your Fit*, FITBIT, https://www.Fitbit.com/compare (last visited Dec. 1, 2015).

12 *Id.*

13 *Meet the App That's All in One, for Everyone*, FITBIT, https://www.Fitbit.com/app (last visited Dec. 1, 2015). The dashboard can also be used without a sensor.

14 *Id.*

15 *Aria*, FITBIT, https://www.Fitbit.com/aria (last visited Dec. 1, 2015).

16 *Tory Burch for Fitbit*, FITBIT, https://www.Fitbit.com/toryburch, (last visited Dec. 1, 2015).

17 Dan Ledger & Daniel McCaffrey, *Inside Wearables: How the Science of Human Behavior Change Offers the Secret to Long-Term Engagement*, ENDEAVOUR PARTNERS 2 (2014), http://endeavourpartners.net/assets/Wearables-and-the-Science-of-Human-Behavior-Change-EP4.pdf. For an overview of the various types of consumer sensor devices, see Peppet, *supra* note 3, at 98-116.

18 Nicole Lee, *Zensorium's 'Being' Is a Fitness Wearable that Promises To Track Your Mood as Well*, ENGADGET (Jan. 4, 2015, 9:40 PM), http://www.engadget.com/2015/01/04/zensorium-being.

19 For a discussion on employer use of health-related sensor data, see *infra* Section I.A.

or calm.[20]

Apps that help measure aspects of health and fitness are growing exponentially as well. According to Google, the "health and fitness" category was the fastest growing app industry segment in 2014.[21] Industry analysts estimate that there are now one hundred thousand mobile health apps available for Android and iOS, twice as many as there were in 2012.[22] The global health and fitness mobile app market, now worth about $4 billion, is expected to multiply six times to $26 billion by 2017.[23] The Food and Drug Administration (FDA) estimates that 500 million smartphone users now use or will soon use at least one health care app.[24]

As described above, there has been a tremendous rise in health and fitness data collection, and new technologies are being developed and brought to market frequently. These technologies present a number of shared legal issues and privacy concerns, but there are also distinct legal issues attending each kind of technology. This Article will focus its discussion on wearable health monitoring sensors, such as those located in devices like the Fitbit as well as those embedded in smart phones and their accompanying mobile apps. These personal health monitors pose a number of privacy concerns. In addition to these more general concerns, the use of fitness tracking devices in the employment setting gives rise to a distinct set of issues and questions. This Article will focus on these special harms that may exist when monitors are used by employers, distinct from the privacy issues that surround the monitors more generally.

A. Health and Fitness Data Collection is on the Upswing

Never have employers had so much new and valuable data about their workforce released to them within such a short time. When employees use wearable sensors to record health and fitness data, employers can often buy and analyze these data for a range of purposes, as described in more detail below. The rapidly increasing collection of health-related data from wearable devices and apps sits at the convergence of three trends: (1) the Internet of Things, (2) the

---

20 Kevin Bullis, *Device Changes Your Mood with a Zap to the Head*, TECH. REV. (Nov. 10, 2014), http://www.technologyreview.com/news/532321/device-changes-your-mood-with-a-zap-to-the-head; *Forward Thinking in Every Sense*, THYNC, http://www.thync.com/about (last visited Dec. 1, 2015).

21 Andy Boxhall, *2014 Is the Year of Health and Fitness Apps, Says Google*, DIGITAL TRENDS (Dec. 11, 2014), http://www.digitaltrends.com/mobile/google-play-store-2014-most-downloaded-apps.

22 *Id.*

23 *Id.*

24 *Mobile Medical Applications*, FOOD & DRUG ADMIN. (June 4, 2014), http://www.fda.gov/Medicaldevices/digitalhealth/mobilemedicalapplications/default.htm#a.

Quantified Self Movement and (3) the rise of the health data platform.

1. The Internet of Things

The Internet of Things (IoT) is the shorthand term given to the increasing interconnectivity of common objects.[25] Examples include refrigerators that detect when you are low on milk and populate grocery lists which pop up on your cell phone and beds that self-adjust to cool you down or heat you up, as needed, and remotely start your coffee maker within a certain time after you get up. By the end of 2015, some experts estimate that there will be twenty-five billion connected devices and that that number will double by 2020.[26] Three and a half billion sensors are in use now, and some predict that there will be trillions of sensors within ten years.[27]

There is a gap, however, between the institutional embrace of the Internet of Things and public comfort levels. In a January 2015 survey by a Nielsen company, fifty-three percent of respondents said they were concerned that their data might be shared without their knowledge or approval—almost as many worried about the risk of security breaches. Of the 4000 survey respondents, fifty-one percent said they were concerned that their data could be hacked by other users.[28] Whether their personal data are shared intentionally or unintentionally, these numbers suggest that just over half of consumers are concerned about the loss of privacy that more interconnectedness may bring.

2. The Quantified Self Movement

The Quantified Self Movement refers to the increasing popular demand for devices that monitor and measure an enormous range of physical data about oneself, including heart rate, weight, blood sugar, sleep patterns, and diet.[29] Monitoring technology takes an increasingly wide range of forms, including shirts embedded with sensors as well as sensors that can be implanted on and under the skin.[30]

---

25 Janna Anderson & Lee Rainie, *The Internet of Things Will Thrive by 2025* (May 14, 2014), www.pewinternet.org/2014/05/14/internet-of-things.

26 *Id*.

27 *TSensors Summit for Trillion Sensor Roadmap*, TSENSORS SUMMIT (2013), http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf.

28 Kim Gaskins, *What's Holding Back the Internet of Things?*, VENTURE BEAT (Jan. 18, 2015, 6:58 AM), http://venturebeat.com/2015/01/18/whats-holding-back-the-internet-of-things.

29 *See, e.g.*, Dawn Nafus & Jamie Sherman, *This One Does Not Go Up to 11: The Quantified Self Movement as an Alternative Big Data Practice*, 8 INT'L J. COMM., 1784, 1788 (2014).

30 *See, e.g.*, Daniel Cooper, *Hexoskin's Smart Shirt Feels Nice, but Can't Tell a Step*

As sensors migrate internally, it may also become harder to turn these sensors off or remove them, making it more difficult for employees to control the flow of health-related data to the outside world. Because these kinds of devices are harder to alter, they are potentially more valuable to employers, less susceptible to employee error, and more likely to raise serious privacy concerns.

3. The Emergence of Health Data Platforms

A third relevant trend is the centralization of fitness data collected from disparate sources through dedicated software platforms. The world's largest electronics manufacturers expect interest in health and fitness monitoring to continue its explosive growth and are making it easier for users to monitor themselves. Apple's Health app allows users to see all of their health and fitness data at a glance. As one observer put it, "you could use devices and apps from different companies—say a Nike FuelBand, a Withings Blood Pressure Monitor, and an iHealth Wireless Smart Gluco-Monitoring System—and have information from all of them gathered in the Apple Health app, which serves as a dashboard for your health and fitness data."[31] Apple's competitor Samsung is also investing heavily in the symbiosis of disparate health and fitness monitors. In 2014, it announced the development of Samsung Architecture for Multimodal Interactions (SAMI), which centralizes data from various health-related apps and devices and makes it accessible to others, perhaps including employer-sponsored collectors.[32]

Apple and Samsung have also introduced devices that complement the health data collection features of this software. Apple's iPhone 6 and iPhone 6 Plus feature an M8 motion co-processor chip that improves the phones' function

---

from a Curl, ENGADGET (Dec. 2, 2014, 12:00 PM), http://www.engadget.com/2014/12/02/hexoskin-hands-on; *see also* Daniel Cooper, *Your Next Smart Shirt will Make You Look Like an Extra from 'Tron,'* ENGADGET (Jan. 6, 2015, 4:56 PM), http://www.engadget.com/2015/01/06/cambridge-consultants-xelflex; Daniel Cooper, *EES Packs Circuits into Temporary Tattoos, Makes Medical Diagnostics Fashionable*, ENGADGET (Aug. 12, 2011, 11:52 PM), http://www.engadget.com/2011/08/12/ees-packs-circuits-into-temporary-tattoos-makes-medical-diagnos; Jon Fingas, *Sticky Sensors Will Monitor Your Body's Organs*, ENGADGET (Dec. 30, 2014, 2:18 AM), http://www.engadget.com/2014/12/30/sticky-organ-sensors.

31 Nicole Lee, *Apple: Putting Doctors, Trainers and Nutritionists in Your Pocket*, ENGADGET (June 3, 2014, 9:17 PM), http://www.engadget.com/2014/06/03/apple-healthkit-fitness.

32 *See* Mark Sullivan, *Samsung Wants 'SAMI' and 'Simband' To Be the Start of a New Biohealth Ecosystem*, VENTURE BEAT (May 28, 2014, 11:37 AM), http://venturebeat.com/2014/05/28/samsung-announces-simband-biosensor-watch-reference-design.

as a fitness monitor. The M8 allows the phones to detect what kind of physical activity the user is engaged in (e.g., running, biking, or walking) and estimate the distance traveled and even the altitude thanks to a built-in barometer.[33] Samsung has introduced the Simband, an open-hardware sensor that can collect a wide range of health and fitness data in conjunction with SAMI.[34] According to Samsung, "the combination of Simband-designed sensor technology and algorithms and SAMI-based software will take individual understanding of the body to a new level—for the first time giving voice to a deeper understanding of personal health and wellness."[35] In early 2014, Samsung also unveiled the first mobile phone with an integrated heart rate monitor, its Galaxy S5.[36] The fact that Samsung and Apple both build fitness sensors into their flagship phones is a powerful indicator that more health data will be collected and potentially used by employers over time. Employers often provide phones to their employees, and Samsung and Apple are the world's leading mobile phone manufacturers.[37]

The aggregation of health data on phones is, in its core function, not that different from the aggregation of movement, sleep, and heart rate data on the Fitbit dashboard or a similar mobile app. On both phones and dedicated health wearables, an app can centralize a number of inputs with the goal of providing a more comprehensive overview of ostensibly related data than any single input could provide. On the Fitbit dashboard, these inputs may come from a Fitbit band, a synched Aria scale, or the user's own typing. Apple and Samsung's platforms coordinate inputs from a wider range of sources.

---

33 Ashley Feinberg, *The iPhone 6's New M8 Chip Makes It a Truly Badass Fitness Tracker*, GIZMODO (Sept. 9, 2014, 1:32 PM), http://gizmodo.com/the-iphones-new-m8-chip-makes-it-a-truly-badass-fitness-1632519058.

34 *See* Nicole Lee, *Samsung Launches A Flexible Platform of Sensors for Wearables*, ENGADGET (May 28, 2014, 2:16 PM), http://www.engadget.com/2014/05/28/samsung-launches-a-flexible-platform-of-sensors-for-wearables. Interestingly, SAMI was developed in part by Luc Julia, a former Apple engineer. *See* Samuel Gibbs, *Samsung's SAMI Project Is Led by Former Siri Engineer from Apple*, GUARDIAN (Nov. 11, 2013, 10:12 AM), http://www.theguardian.com/technology/2013/nov/11/samsungs-sami-project-siri-engineer-apple.

35 Michelle Maisto, *Apple, Samsung Taking Different Roads to Consumer Health Empowerment*, EWEEK (June 9, 2014), www.eweek.com/mobile/apple-samsung-taking-different-roads-to-consumer-health-empowerment.html.

36 Michelle Maisto, *Samsung Unveils Galaxy S5, Gear Fit, Galaxy Gear 2, Gear 2 Neo at MWC*, EWEEK (Feb. 25, 2014), http://www.eweek.com/mobile/slideshows/samsung-unveils-galaxy-s5-gear-fit-galaxy-gear-2-gear-2-neo-at-mwc.html.

37 Press Release, Gartner, Inc., Gartner Says Smartphone Sales Surpassed One Billion Units in 2014 (Mar. 3, 2015), http://www.gartner.com/newsroom/id/2996817.

II. EMPLOYERS HAVE UNPRECEDENTED ACCESS TO EMPLOYEES' HEALTH AND FITNESS DATA

Employers have every incentive to collect as much data as they may, especially when doing so increases profitability. Fitbit invites employers to adopt its "Fitbit Wellness" program to track employees individually and in groups, "potentially reducing health care costs."[38] Many employers encourage the use of wearable monitors as part of their corporate wellness programs, often in the hope that having healthier employees will help them negotiate discounted health care rates.[39] Minimizing health insurance costs is only one example of how employee data can improve the bottom line. Using health data to inform hiring and promotion decisions is another. The legality of the use of employee data is an increasingly important question in employment and privacy law.

The explosive growth of wearable device ownership makes it easier than ever for employers to collect health and fitness data about their employees. The people most likely to use those devices are those whom employers are most interested in evaluating. People in their late twenties and early thirties have the highest rates of ownership, with people age twenty-five to thirty-four accounting for twenty-five percent of survey respondents between age twenty-five to thirty-four reporting that they have an activity tracker.[40] Conversely, the lowest rates of ownership are, as one might expect, among those over sixty-five, with only seven percent of activity trackers owned by that group.[41]

The rates of health tracker ownership coincide nicely with the statistical likelihood of workplace influence. The group most likely to own a fitness tracker is also the group most likely to be filling junior management positions, while the group that is least likely to have these devices is most likely to be retiring from the workplace altogether. Younger workers are also more vulnerable to the lack of protection for sensor-generated health data because they are more likely to be in the workforce longer than older workers and therefore may provide more data over time. In that sense, the age cohort with the most to lose from employer misuse of health and fitness data is the one most susceptible to that misuse.

---

38 *Fitbit Wellness*, FITBIT. http://www.Fitbit.com/Fitbit-wellness (last visited Dec. 1, 2015).

39 Aditya Kaul & Clint Wheelock, *Wearable Devices for Enterprise and Industrial Markets: Executive Summary*, TRACTICA 3 (2015), https://www.tractica.com/wp-content/uploads/2015/04/WDEI-15-Executive-Summary.pdf; *see also* discussion *infra* Section II.A (explaining the financial incentives that encourage employers to establish wellness programs).

40 Ledger & McCaffrey, *supra* note 17, at 3.

41 *Id.*

A. New Technology Facilitates Employee Health Data Collection

Employers are starting to collect a wide range of data from more ubiquitous and often mandatory wearable devices. The collection of health and fitness data is part of a larger trend toward electronic monitoring of individual employees. Hitachi, for example, now offers employers the Business Microscope, a kind of advanced employee security badge embedded with infrared sensors, a microphone sensor, and a wireless communication device. When two employees wear these badges within a certain distance of each other, the badges recognize each other, record face time and body and behavioral data, and send them to a server.[42] The badges send management data about who talks to whom, how often, where, and with how much energy. It also tells employers how much time each employee spends out of their seats. A similar employee monitoring badge developed by Sociometric Solutions includes a microphone that assesses the tone of voice the employee uses as well as an infrared beam that determines the speaker's position relative to other badge-wearing employees.[43] The British grocery chain Tesco uses an armband containing a Motorola device to monitor its employees' productivity and to track when they take breaks.[44]

Employers have strong financial incentives for adopting these monitoring technologies, both in the form of increased productivity and lower costs. One journalist notes that "while privacy concerns are an obvious issue," the system has been shown to improve productivity.[45] One retail seller reported a fifteen percent increase in average sales per customer after using the badges for ten days.[46] Another company was recently sued for firing an employee who uninstalled a required tracking app from her work phone.[47]

Another financial incentive for monitoring employees is a potential reduction in health care costs. This incentive stems from employees' use of health and fitness data sensors like the Fitbit and sensor-enabled smartphones. For example, BP offers a program by which employees can cut $1200 from their

---

42 Victoria Young, *Wearable Device Monitors Employee Productivity*, PSFK, (Feb. 10, 2014), http://www.psfk.com/2014/02/wearable-employee-productivity-tracker.html.

43 Vivian Giang, *Companies Are Putting Sensors on Employees To Track Their Every Move*, BUS. INSIDER (Mar. 14, 2013, 6:23 PM), http://www.businessinsider.com/tracking-employees-with-productivity-sensors-2013-3.

44 Claire Suddath, *Tesco Monitors Employees with Motorola Armbands*, BLOOMBERG (Feb. 13, 2013), http://www.bloomberg.com/bw/articles/2013-02-13/tesco-monitors-employees-with-motorola-arm-bands.

45 Victoria Young, *Hitachi Is Using Data Visualization To Increase Inter-Company Communication and Efficiency*, PSFK (Feb. 10, 2014), http://www.psfk.com/2014/02/wearable-employee-productivity-tracker.html.

46 *Id.*

47 Complaint at 3-4, Arias v. Intermex Wire Transfer, LLC, No. S1500CV284763 (Cal. Sup. Ct. May 5, 2015), 2015 WL 2254833.

annual insurance bills in exchange for wearing a Fitbit and logging a sufficient amount of physical activity.[48] When BP introduced this free Fitbit program in 2013, 14,000 employees, 6000 spouses, and 4000 retirees signed up.[49] Like other employers, BP faces rising health care costs and is looking for ways to reduce them. Although some may question the genuineness of an employer-sponsored discount on health insurance rates, insurers are starting to offer similar discounts directly. For example, John Hancock Insurance offered customers up to a fifteen percent discount on their insurance rates in exchange for healthful activity as measured by the Fitbits these customers agreed to wear.[50]

Employers like BP, Cigna, and Autodesk also offer their employees the Fitbits for free or at substantially reduced rates in a program that they can describe as a "win-win" for both sides.[51] The employers have a vested interest in their employees' health, and the employees get a significant discount on a popular device. One effect of employer-monitored wearables may be increased or longer use of the device.[52] As noted in a recent blog post, "[B]y encouraging employees to use their personal fitness devices in the right way, companies can motivate employees to continue using their wearables, and achieve lasting health benefits."[53]

Lowering health insurance costs is a powerful motivation for employers to provide fitness sensors. If enough of their employees wear Fitbits or similar devices, presumably increasing their fitness, employers may be able to negotiate lower health insurance costs because of the likely decrease in claims for their healthier employees. For example, Appirio, a Bay Area startup, negotiated a $300,000 discount on its $5 million insurance costs by agreeing to share employee health data with its insurer and showing that the staff's health was improving.[54] Employees who lost weight using a fitness program that included uploading activity on their Fitbits shared that information on the company's internal social network, and the program became increasingly popular. Forty

48 Adam Satariano, *Wear This Device So the Boss Knows You're Losing Weight*, BLOOMBERG (Aug. 21, 2014, 1:26 PM), http://www.bloomberg.com/news/articles/2014-08-21/wear-this-device-so-the-boss-knows-you-re-losing-weight.

49 Olson & Tilley, *supra* note 1.

50 Tara Siegel Bernard, *Giving out Private Data for Discount in Insurance*, N.Y. TIMES (Apr. 8, 2015), http://www.nytimes.com/2015/04/08/your-money/giving-out-private-data-for-discount-in-insurance.html.

51 *See* David Nield, *Employee Wellness Programs Now One of Fitbit's Fastest Growing Areas*, DIGITAL TRENDS (Apr. 19, 2014), http://www.digitaltrends.com/mobile/employee-wellness-programs-now-one-Fitbits-fastest-growing-areas.

52 *See* Ledger & McCaffrey, *supra* note 17, at 7.

53 Panpan Wang, *Employers Key to Helping Consumers Take Advantage of Wearables Trend*, JIFF (Sept. 16, 2014), http://www.jiff.com/blog/2015/2/17/mqo9ufzmh66jkqtfanukc3hbqc3pyw.

54 Satariano, *supra* note 48.

percent of Appirio's approximately 1000 employees upload their fitness data via their Fitbit devices.[55] Their progress was persuasive to the company's insurer. According to Appirio's CEO, Chris Barbin, "We had an initial batch of data about people who had lost weight, and people who had moved from high risk to moderate risk. When we could show all that information to our insurer, that's pretty powerful." Barbin noted that there are privacy protections for employees' uploaded fitness data, although he has not disclosed the specific parameters of those protections.[56]

Insurers are working closely with employers to facilitate programs like these. United Health Group, Humana, Cigna, and Highmark have all developed programs that help their employer clients integrate wearable devices like the Fitbit into the workplace.[57] While encouraging preventive measures is nothing new, adopting wearable fitness sensors can help boost incentives for employees to upload proof of their physical activity.

This tech-assisted approach to employee wellness fits into a general trend of increased spending on health programs at work. According to one study, spending on corporate wellness incentives more than doubled between 2009 and 2014, with corporations now spending an average of $594 per employee annually on such programs.[58] Wearable technology will continue to play an important role in this trend. By 2018, analysts predict that a third of fitness-tracking device sales will come from corporate wellness programs.[59]

B. Providers and Platforms Help Aggregate Employee Health Data

In coming years, the amount of health-related information that can transfer from an employee to a wearable sensor will increase. Medical professionals champion the use of health data sensors, in part to improve the quality of medical treatment as doctors spend less time with patients than they have in the past.[60] Many predict that implantable or wearable sensors will send biometric data to a smartphone, continually supplementing a database of information that can help

---

55 *Id.*

56 *Id.*

57 *Id.*

58 *Health Care Survey Finds Spending on Corporate Wellness Incentives To Increase 15 Percent in 2014*, FIDELITY (Feb. 20, 2014), http://www.fidelity.com/inside-fidelity/employer-services/health-care-survey-finds-spending (describing an increase in spending of "more than double the average of $260" reported in 2009).

59 Adrian Kingsley-Hughes, *Wearables and Health Insurance: A Health Bar over Everyone's Head*, (Aug. 26, 2014,10:25 AM), http://www.zdnet.com/article/wearables-and-health-insurance-a-health-bar-over-everyones-head.

60 *See, e.g.*, Anick Jesdanun, *Doctors Say Fitness Trackers, Health Apps Can Boost Care*, PHYS.ORG (Feb. 20, 2015), http://phys.org/news/2015-02-doctors-trackers-health-apps-boost.html.

monitor health conditions.[61] According to Nathan Cortez, "Smartphones already are replacing stethoscopes and pagers as the most ubiquitous physician accessory."[62] Professor Cortez has created a typology of mobile health apps, many of which rely on sensors, currently in use.[63] He categorizes them as follows:

(1) Connectors, which include apps that "connect smartphones and tablets to FDA-regulated devices, thus amplifying the devices' functionalities."[64]
(2) Replicators, which "turn the smartphone or tablet itself into a medical device by replicating the functionality of an FDA-regulated device."[65]
(3) Automators and Customizers, which "use questionnaires, algorithms, formulae, medical calculators, or other software parameters to aid clinical decisions."[66]
(4) Informers and Educators, encompassing "educational apps that primarily aim to inform and educate."[67]
(5) Administrators, which "automate office functions" including "scheduling patient appointments."[68]
(6) Loggers and Trackers, which "allows users to log, record and make decisions about their general health and wellness."[69]

It is this final category that is most relevant for purposes of this Article. The growth and development of the other categories, however, signals the increasing importance of mobile health technology in general.

The growing demand for health and fitness data will be driven as much by employers as by the medical profession. Device manufacturers and app developers recognize the importance of employers as a revenue stream. Fitbit began selling data in bulk to employers in 2010 along with software that facilitates the translation of data.[70] Through its Fitbit Wellness program, Fitbit now partners with "thousands" of employers to provide its wearable devices at a

---

61 *See* ERIC TOPOL, THE CREATIVE DESTRUCTION OF MEDICINE 162-63 (2012) (describing hypothetical nanosensor monitoring of patients' blood to detect markers of heart disease or cancers for those at high risk of such diseases).

62 Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1177 (2014).

63 *Id.*

64 *Id.* at 1182.

65 *Id.* at 1184.

66 *Id.* at 1186.

67 *Id.* at 1188.

68 *Id.* at 1189.

69 *Id.*

70 *See* Parmy Olson, *Jawbone Jumps into Employee Fitness Monitoring*, FORBES (Dec. 11, 2014, 7:48 AM), http://www.forbes.com/sites/parmyolson/2014/12/11/jawbone-employee-fitness-monitoring.

discount along with software that allows the employers to see how active certain employees are.[71] Its website promises that employers in the program can "monitor individual, team and company-wide progress."[72] The benefits of adopting a Fitbit Wellness program, according to the site, include the ability to "create a culture of well-being," "increase employee productivity," "improve employee health status," and "boost acquisition and retention."[73] In 2014, Fitbit's CEO announced that sales to employers are "one of the fastest-growing parts of Fitbit's business."[74] Fitbit's competitors are developing similar programs. In late 2014, Jawbone introduced UP for Groups, a program through which employers can buy Jawbone fitness trackers in bulk at a discount and use centralized software to track their use in the aggregate.[75]

Previously, employers could track their employees' activity, but only through an application programming interface (API).[76] Employers don't have to go through device manufacturers like Fitbit or Jawbone, however, to collect health-related information about their employees. Startups including Pact, WelBe, and Jiff also sell software that allows employers to track and collect this kind of data from any wearable device.[77] WelBe's website, for example, suggests that its software can monitor how much employees sleep, eat, drink, and exercise.[78] It coordinates input from sources including Fitbit, Garmin, MyFitnessPal, RunKeeper, and Jawbone.[79] WelBe offers what it ominously calls "wellbeing coordinators"—which presumably used to be human resources managers—the ability to "create aggregated biometric reports on the fly and take a deep dive into data on employees' activity levels, financial fitness, challenge activities, and nutritional health."[80] Data aggregators such as TicTrak and Foxing also collect information from various fitness trackers.[81]

App developers find it increasingly easy and rewarding to generate data that

---

71 *Id.*

72 *Fitbit Wellness*, *supra* note 38.

73 *Id.*

74 *See* Nield, *supra* note 51.

75 *See* Olson, *supra* note 70.

76 *Id.*

77 *Id.*

78 WELBE, https://www.welbe.com (last visited Dec. 1, 2015). On this site, an embedded video without narration entitled "How Do You Live Welbe?" shows a young woman whose every move, from the moment she wakes up in the morning, appears to be recorded. It is not clear exactly how each of these data points is being recorded, as we see her with a wearable device, entering information into an app on her phone .

79 Tom Rath, *A New Version of Eat, Move, Sleep, and the Welbe App*, O.C. TANNER (Jan. 19, 2015), http://blog.octanner.com/editor-picks/a-new-version-of-eat-move-sleep-and-the-welbe-app.

80 *See* WELBE, *supra* note 78.

81 *See* Ledger & McCaffrey, *supra* note 17, at 4.

can be centralized and transferred in this way. For example, Apple's introduction of HealthKit, in June 2014, simplified the aggregation and transfer of health related data. HealthKit is a tool that helps developers create apps that draw on a user's centralized health and fitness data, effectively allowing them to share data with and import data from other HealthKit-enabled apps.[82]

While the most direct means of data collection at work is to use employer-provided devices and apps, employers could also collect data generated by employees' own devices. Employers have already shown a willingness to use employees' personal technology to their advantage, blurring the line between personal data and workplace device. The "Bring Your Own Device" (BYOD) movement has gained ground quickly.[83] Courts have yet to fully define the extent to which employers may legally collect non-work-related data from these devices.

C. *Using Employee Health Data To Inform Employment Decisions Creates Potential Legal and Ethical Hazards*

There is ample potential for employer misuse of current and future employees' health and fitness data.[84] These data could inform employment decisions in nearly unlimited ways. As Professor Peppet points out, smartphone sensors can provide data from which employers can infer "a user's mood, stress levels, personality type, bipolar disorder, demographics (e.g., gender, marital status, job status, age); smoking habits, overall well-being, progression of Parkinson's disease, sleep patterns, happiness, levels of exercise, and types of physical activity or movement."[85] It is easy to imagine a scenario where an

---

82 *The HealthKit Framework*, APPLE, INC. (Nov. 19, 2015), https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/index.html#//apple_ref/doc/uid/TP40014707.

83 Anisha Mehta, *"Bring Your Own Glass": The Privacy Implications of Google Glass in the Workplace*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 607, 607-08 (2014).

84 *See, e.g.*, Karen Levy, *Relational Big Data*, 66 STAN. L. REV. ONLINE 73, 77 (2013) ("Fast-growing workplace wellness monitoring programs frequently use health indicators and behavioral data (derived, for instance, from a digital pedometer) to let employers and insurers keep tabs on the health of their workforce . Highly mobile employees like truck drivers . . . are increasingly monitored via fleet management and dispatch systems that transmit data about their driving habits, fuel usage, and location to a central hub in real time—practices that have engendered deep concerns about driver privacy and harassment."); Thierer, *supra* note 3, at 55 (noting that "new datasets" derived from interconnected devices "might be used . . . by employers for job-related purposes, or even by insurers to adjust user premiums"). At least one Canadian lawyer has introduced Fitbit data as evidence of decreased physical activity in a personal injury lawsuit . Samuel Gibbs, *Court sets legal precedent with evidence from Fitbit health tracker*, THE GUARDIAN (Nov. 18, 2014, 11:03 AM), http://www.theguardian.com/technology/2014/nov/18/court-accepts-data-Fitbit-health-tracker.

85 Peppet, *supra* note 3, at 115-16 (footnotes omitted).

employer, having to decide which of two candidates to promote, reviews each candidate's sleep patterns, physical activity, calorie intake, or mood—any or all of which can be monitored and measured remotely—and decides based at least in part on these data. When employers use the health and fitness data they collect to make employment decisions, including hiring and promotion, there is cause for concern.[86]

As discussed further in the next Part, the legal frameworks we rely on to prohibit discrimination are of little use here. Evaluating an employee for a promotion based on the employer's assessment of the likelihood that the employee will develop an unspecified health condition later in life, for example, based on the candidate's monitored physical activity levels, would not invoke disability law because no specific disability is invoked or perceived.[87] Making employment choices based even in part on sleep patterns, nutritional intake, or smoking—all of which can be measured by mobile sensors—may look like discrimination to a non-lawyer. Lawyers might analyze a potential discrimination claim by asking whether the employee was targeted because of membership in a protected class under Title VII of the Civil Rights Act,[88] such as race or religion, or a disability as defined by the Americans with Disabilities Act (ADA).[89] However, non-lawyers may not use that analytical framework. Treating an employee or job candidate differently because of physical activity levels or sleep patterns—conditions which may correlate to lower productivity levels and/or higher health insurance costs in the future—may seem wrong to a non-lawyer and indeed may well be unethical.[90] However, federal anti-discrimination laws do not protect employees against decisions made on these bases; rather, these laws only reach employees who fall within a protected class.[91]

---

86 *Id.* at 118-119 ("Impulsivity and the inability to delay gratification – both of which might be inferred from one's exercise habits – correlate with alcohol and drug abuse, disordered eating behavior, cigarette smoking, higher credit-card debt, and lower credit scores. Lack of sleep – which a Fitbit tracks – has been linked to poor psychological well-being, health problems, poor cognitive performance, and negative emotions such as anger, depression, sadness, and fear. Such information could tip the scales for or against" a job candidate) (citations omitted); *see also* Dennis D. Hirsch, *That's Unfair! Or is it? Big Data, Discrimination and the FTC's Unfairness Authority*, 103 KY L.J. 345, 350-352 (2014-2015) (describing potential discrimination resulting from use of health-related Big Data); Jessica L. Roberts, *Protecting Privacy to Prevent Discrimination*, 56 WM. & MARY L. REV. 2097, 2122 (May 2015) (noting potential for discrimination when access opens to private information).

87 Peppet, *supra* note 3, at 125-26.

88 Civil Rights Act of 1964, Pub. L. No. 88-352, § 703, 78 Stat. 241, 255-57 (1964) (codified as amended at 42 U.S.C. § 2000e-2 (2012)).

89 Americans with Disabilities Act (ADA) of 1990, Pub. L. No. 101-336, § 102(a), 104 Stat. 327, 331-32 (codified as amended at 42 U.S.C. § 12112(a) (2012)).

90 *See supra* note 86 and accompanying text.

91 *See, e.g.*, ADA § 102(a).

There are other risks as well. Employers who collect health and fitness data are susceptible to security breaches, possibly leading to the unauthorized distribution of data. Such security breaches are on the rise. According to one survey, there were over 300,000 reported cases of medical identity theft in 2013, a nineteen percent increase over the previous year. [92]

There is also the danger that in-house staff may manipulate the data collected for a variety of reasons. Employees are unlikely to check the accuracy of the health-related data their employers collect. Most people do not verify the accuracy of their health records at all. In a 2013 survey, fifty-six percent of respondents admitted that they do not check their medical records to determine if the health information is accurate at all.[93]

III. FEDERAL LAW DOES TOO LITTLE TO PROTECT EMPLOYEE HEALTH DATA

Mobile sensors can gather various types of data. These include the kind of direct health data that a medical device might record (such as blood pressure or heart rate) as well as non-health data, such as the employees' specific location data (for example, using a GPS). This Article examines the legal protection available to employees concerning the use of their health-related data. I believe that the greatest concerns lie with the possible employer misuse of extrapolated or indirect health data such as physical activity, sleep patterns, and heart rate.

While several federal laws appear to prohibit employers' potential misuse of health and fitness data, significant gaps remain in the federal protection of these data.[94] Many federal agencies and laws might address this growing problem, but none do so effectively. While states have a variety of data privacy laws, this Article focuses instead on the shortcomings of federal law in the protection of employees across the country. Adverse employment decisions using these data may fall outside existing federal anti-discrimination protections; accordingly, it is critical to examine the extent to which federal law otherwise protects employees from employer decisions of this kind.[95]

92 *2013 Survey on Medical Identity Theft*, PONEMON INST. 2 (2013), https://clearwatercompliance.com/wp-content/uploads/2013/10/2013-Medical-Identity-Theft-Report-FINAL.pdf.

93 *Id.* at 13.

94 As discussed *infra* in Section III.B.

95 State laws can provide important protections as well, but the extent to which they may do so falls outside the scope of this Article.

A. Employees May Have No Reasonable Expectation of Privacy in Sensor-Generated Health Data

An important preliminary question is whether there is any right of privacy in health-related information beyond specific regulatory protections.

Some have observed that consumers have ever-decreasing expectations of privacy.[96] The increasing use of personal devices at work is further eroding these expectations of privacy.[97] Recent studies show, however, that many people still fear losing privacy, especially as it becomes easier to transmit information through technology. In a 2015 survey, privacy and security were respondents' top concerns about the Internet of Things.[98] More than half expressed concern that their data might be shared without their knowledge or approval. In addition, most people expect their health data to be kept somewhat private by HIPAA,[99] which may weigh in favor of finding that society values data privacy more than HIPAA actually protects it.

When employers give their employees electronic devices for work purposes, the employers arguably have greater legal access to the data on those devices than anyone else. In *City of Ontario v. Quon*, the Supreme Court held that public employees using devices provided by their employers for work purposes have little reasonable expectation of privacy in doing so.[100] While *Quon* concerned a government employer, the Court made it clear that the rapid pace of technological change would have made a sweeping holding on the scope of technological privacy at work imprudent. "Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices," wrote Justice Kennedy in the majority opinion.[101] "A broad holding concerning employees' privacy

---

96 *See, e.g.*, Kate Murphy, *We Want Privacy, but Can't Stop Sharing*, N.Y. TIMES (Oct. 4, 2014), http://www.nytimes.com/2014/10/05/sunday-review/we-want-privacy-but-cant-stop-sharing.html.

97 Stephen Wu, *Employee Privacy in the Dawn of the Mobile Revolution*, RECORDER (Feb. 22, 2013), http://www.therecorder.com/id=1202588380082/Employee-Privacy-in-the-Dawn-of-the-Mobile-Revolution?slreturn=20151027170150.

98 *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers*, PONEMON INST. 1 (2015), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rt_privacy_and_security_in_a_connected_life.pdf.

99 *See, e.g.*, *National Consumer Health Privacy Survey 2005: Executive Summary*, CALIFORNIA HEALTHCARE FOUNDATION 1 (2005), http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/PDF%20C/PDF%20ConsumerPrivacy2005ExecSum.pdf.

100 560 U.S. 746, 747 (2010).

101 *Id.* at 748.

expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted."[102]

The Supreme Court has yet to issue a detailed ruling as to whether there is a reasonable expectation of privacy over the health and fitness data employers collect from their employees. Since *Quon* was decided in 2010, however, lower courts have grappled with the extent of privacy in connection with electronic devices. Most of the leading cases have come from the Bay Area, where both Fitbit and Jawbone are headquartered. In 2014, the Northern District of California dismissed an employee's claims that his former employer violated the Wiretap Act, Stored Communications Act, California anti-hacking and privacy laws, or invaded his privacy by accessing the employee's electronic communications through an Apple account he had created in connection with employer-provided devices.[103] The facts of that case are unusual, however, in that the employee caused the communications to be transmitted to the employer through his voluntary actions, undercutting any expectation of privacy he may have had.[104] The same court allowed a class action lawsuit to proceed against Google for sharing customers' personal information with app vendors without the customers' authorization.[105] That decision may undercut the ability of employers, or of Fitbit or Jawbone, to share employees' fitness data with a third party, depending on its final resolution.

A final case that privacy scholars will follow as it develops is *Arias v. Intermex Wire Transfer*. In May 2014, Intermex Wire Transfer allegedly fired Myrna Arias after she uninstalled an app called Xora, which tracked her location twenty-four hours a day, from her work-issued phone.[106] In May 2015, Arias sued Intermex for invasion of privacy among other claims.[107]

In the absence of binding precedent on the specific issue of employee privacy in

---

102 *Id.* at 760.

103 Sunbelt Rentals, Inc. v. Victor, 43 F. Supp. 3d 1026 (N.D. Cal. 2014).

104 *Id.* at 1035 ("The facts alleged demonstrate that [Victor, the employee] failed to comport himself in a manner consistent with objectively reasonable expectation of privacy. By his own admission, Victor personally caused the transmission of his text messages to the Sunbelt iPhone by syncing his new devices to his Apple account without first unlinking his Sunbelt iPhone. As such, even if he subjectively harbored an expectation of privacy in his text messages, such expectation cannot be characterized as objectively reasonable, since it was Victor's conduct that directly caused the transmission of his text messages to Sunbelt in the first instance.").

105 Svenson v. Google, Inc., No. 13-cv-04080-BLF, 2015 WL 1503429 (N.D. Cal. Apr. 1, 2015); *cf. In re* Zynga Privacy Litig., 750 F.3d 1098 (9th Cir. 2014) (dismissing class action claims against Facebook and Zynga because users' record information conveyed to third parties was not substantive communication as protected by certain federal statutes).

106 Complaint at 3-4, Arias v. Intermex Wire Transfer, LLC, No. S1500CV284763 (Cal. Sup. Ct. May 5, 2015), 2015 WL 2254833.

107 *Id.* at 4-5.

health-related data collected from mobile sensors, the protections afforded by specific federal regulation, or lack thereof, become even more important.

B. Federal Regulation of Health and Fitness Data Collection Is Fragmented and Insufficient

Americans have a general sense that their personal health information should be secure. Doctors' offices regularly present us with HIPAA notices that provide a sense of reassurance about the privacy of our health records. HIPAA does not adequately protect the kind of health and fitness data generated by popular health and fitness devices and apps nor do any of several other federal laws that might at first appear to protect these data, as discussed in more detail below. These gaps in regulatory coverage deserve greater scholarly and public attention.

1. The Health Insurance Portability and Accountability Act

HIPAA was designed to protect the confidentiality of patients' health information.[108] HIPAA, however, does not protect the kind of health and fitness data that wearable technology or fitness apps might collect.[109] When a Fitbit or iPhone app tells an employer how much an employee has exercised, what her heart rate is, or how high her blood sugar levels are, those data do not fall within the scope of HIPAA protection.

According to the U.S. Department of Health and Human Services (HHS), HIPAA "provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information."[110] The "covered entities" include health care providers, health plans (including insurers and health maintenance organizations (HMOs)), and health care "clearinghouses" that translate health information from one format to another.[111] Certain HIPAA laws also apply to the "business associates" that covered entities hire to help them carry out health care functions. HIPAA only restricts what covered entities and their business associates can do. Other entities and individuals are not so restricted.

Additionally, HIPAA protects "[i]ndividually identifiable health

---

108 The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

109 *See* Timothy S. Hall, *The Quantified Self Movement: Legal Challengers and Benefits of Personal Biometric Data Tracking*, 7 AKRON INTELL. PROP. J. 27, 29-30 (2014).

110 *Understanding Health Information Privacy*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding (last visited Dec. 1, 2015).

111 45 C.F.R § 160.103 (2015).

information," which is a subset of "health information."[112] "Health information" is defined as:

> any information, including genetic information, whether oral or recorded in any form or medium, that
> (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.[113]

The statute goes on to define "individually identifiable health information" as the "subset of health information" that:

> (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
> (i) That identifies the individual; or
> (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[114]

Given these parameters, the kind of health-related data collected by mobile sensors such as Fitbits, smartwatches, and phones could fall under the definition at least of "health information" if it is "received" by a "health plan" or "employer." As Professor Hall has observed, however, the "disclosure of individually identifiable biometric data by the company that manufactures the device, sells the app, or runs the website aggregating the data does not violate HIPAA's Privacy Rule as it currently stands."[115] In other words, if the data are passed from the individual to a third party that is not a "health care provider, health plan, employer, or health care clearinghouse" nor an agent for any such entity, the data fall outside of the statutory HIPAA protections. App

112 *Id.*
113 *Id.*
114 *Id.*
115 *See* Hall, *supra* note 109, at 30.

manufacturers and website managers may qualify as such third parties and therefore may not be bound by HIPAA.

Another potential flaw in HIPAA's protection scheme is its limitation to "individually identifiable" data. When such data are aggregated for export and analysis, it arguably loses HIPAA protection because it is no longer individually identifiable. On the other hand, employers could use these data to infer a great deal about individual users; in essence, the data could be re-identified, or re-engineered to link back to an individual person.[116] This process, also known as "sensor fusion," is now commonly used to collate and synthesize data about a single individual from multiple sources.[117] When HIPAA was passed in 1996, it was more difficult to re-identify data that had been unlinked to an individual user, but recent technological developments have made it easier to re-identify data.[118] The expansion of data available about each of us from a range of sources, including where we take our phones and what websites we visit, facilitates the re-identification process. Data analysts and computer scientists are continually finding new ways to re-identify data by combining various de-identified data pieces with such public information.[119] Whether HIPAA protects such re-identified data has yet to be determined in court.

A final inadequacy of HIPAA as a source of protection for health data is that it provides no private right of action to plaintiffs who feel their privacy rights have been violated under the act. The Clinton Administration supported the inclusion of a private right of action for patients under HIPAA, but Congress chose not to act on these recommendations.[120] Only the HHS Office for Civil Rights may investigate and impose civil and criminal penalties against a health care provider for violations of HIPAA.[121]

---

116 N. Nina Zivanovic, *Medical Information as a Hot Commodity: The Need for Stronger Protection of Patient Health Information*, 19 INTELL. PROP. L. BULL. 183 (2015); *see also Re-Identification: Concerning the Re-Identification of Consumer Information*, ELEC. INFO. PRIVACY CTR., https://epic.org/privacy/reidentification (noting that "data can easily be re-identified, such that the sensitive information may be linked back to an individual.") (last visited Dec. 1, 2015).

117 *See, e.g.*, T. Phan et al., *Sensor Fusion of Physical and Social Data Using Web SocialSense on Smartphone Mobile Browsers*, INST. ELECTRICAL & ELECTRONIC ENGINEERS 1 (2014), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6866555&tag=1.

118 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1706 (2010).

119 Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1841 (2011).

120 Joshua D.W. Collins, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, 222-23 (2007).

121 *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164); *see also* Acara v. Banks, 470 F.3d 569, 571 (5th Cir. 2006) (holding no private cause of action for disclosure of PHI

2. The Americans with Disabilities Act Amendments Act

The Americans with Disabilities Act Amendments Act (ADAAA) expands the ADA's protections against employment discrimination on the basis of an actual or perceived disability.[122] Much of the fitness data that sensors generate and employers collect, however, neither constitutes nor correlates with a disability as defined under the ADAAA.[123]

The ADAAA might limit employers' data collection practices in other ways, however. As noted earlier, the drugstore chain CVS requires its employees to submit to personal health data collection or to pay a fine. Is this kind of disclose-or-pay requirement legal? Current case law suggests that it is.[124] One legal barrier might be the ADAAA's provision that employers cannot make "disability-related" inquiries or require prospective or current employees to undergo medical examinations unless they are job-related or subject to a business necessity exception. An inquiry is "disability-related" if an individual's response to the inquiry could reasonably be expected to disclose the presence of a protected disability. Once employment begins, the employer can make disability-related inquiries or require employees to submit to medical examinations only if they are "job-related and consistent with business necessity."[125]

The ADAAA provides a safe harbor for employers' medical testing requirements in three situations, generally in connection with health insurance plans. Employers may make disability-related inquiries or require employees to submit to medical examinations in the following situations:

(1) an insurer, hospital or medical service company, health maintenance organization, or any agent, or entity that administers benefit plans, or

---

during a deposition); Univ. of Colo. Hosp. v. Denver Pub. Co., 340 F. Supp. 2d 1142, 1145 (D. Colo. 2004) (finding no HIPAA private cause of action because the statute created enforcement means for aggrieved persons); O'Donnell v. Blue Cross Blue Shield of Wyo., 173 F. Supp. 2d 1176, 1179-80 (D. Wyo. 2001) (holding no express or implied private cause of action exists under HIPAA).

122 Americans with Disabilities Act Amendments Act (ADAAA) of 2008, Pub. L. No. 110-325, § 5(a), 122 Stat. 3553, 3557 (codified as amended at 42 U.S.C. § 12112(a) (2012)).

123 Peppet, *supra* note 3 at 125-26 (noting that, for example, one's heart rate, on its own, does not necessarily indicate a "disability" as defined by statute. Nor does calorie expenditure, daily activity, or most of the other data commonly recorded by wearable health devices discussed in this article.).

124 *See supra* notes 100-107 and accompanying text.

125 42 U.S.C. §12112(d)(4)(A) (2012); 29 C.F.R. §1630.14(c) (2015).

> similar organizations from underwriting risks, classifying risks, or administering such risks that are based on or not inconsistent with State law; or
>
> (2) a person or organization covered by this chapter from establishing, sponsoring, observing or administering the terms of a bona fide benefit plan that are based on underwriting risks, classifying risks, or administering such risks that are based on or not inconsistent with State law; or
>
> (3) a person or organization covered by this chapter from establishing, sponsoring, observing or administering the terms of a bona fide benefit plan that is not subject to State laws that regulate insurance.[126]

None of these safe harbor provisions may be used as a subterfuge to avoid the underlying anti-discriminatory purposes of the ADAAA.[127]

At least one court has ruled that employers may subject employees to a penalty for failing to submit to health screenings without violating the ADAAA. In 2012, the Eleventh Circuit Court of Appeals decided that Florida's Broward County did not run afoul of the ADAAA when it deducted $20 from each bi-weekly paycheck of employees who refused to submit to a wellness program.[128] The county's wellness program required employees to complete both a confidential health risk assessment questionnaire and a confidential biometric screening. An employee, Bradley Seff, claimed that these requirements violated the ADAAA's prohibitions against required medical screenings. His claim resulted in a class-action lawsuit against the county.

The Court of Appeals affirmed the District Court's decision in favor of Broward County, finding that its wellness program fell within the ADAAA's safe harbor provision because it was a term of the county's benefit plan even though the wellness program was not a formal, written term of the county's plan.[129] Neither the District Court nor the Court of Appeals addressed the question of whether the $20 surcharge for noncompliance in each pay period made the program involuntary. This precedent suggests that the ADAAA will not limit employers' ability to require employees to submit health and fitness data as a condition of employment.

---

126 42 U.S.C. § 12201(c) (1)-(3) (2012). Paragraphs (1), (2), and (3) "shall not be used as a subterfuge to evade" the underlying anti-discriminatory purposes of the ADAAA.

127 *Id.* at (c)(3).

128 Seff v. Broward Cnty, 691 F.3d 1221 (11th Cir. 2012).

129 *Id.* at 1224 (holding that the employee wellness program need not be "explicitly identified in a benefit plan's written documents to qualify as a 'term' of the benefit plan within the meaning of the ADA's safe harbor provision.").

Since *Seff*, courts have started to consider the extent of employees' rights in biometric data in litigation brought by the Equal Employment Opportunity Commission (EEOC) over corporate wellness programs. For example, in September 2014, the EEOC sued Flambeau, Inc., a Wisconsin-based plastics manufacturer, after Flambeau declined to pay any of the medical insurance costs for an employee who refused to complete certain biometric tests and a health risk assessment.[130] Compliant Flambeau employees, according to the EEOC, were only required to pay twenty-five percent of their premium cost.[131] The EEOC had filed a similar lawsuit the previous month against another Wisconsin employer, Orion Energy Systems, which allegedly fired an employee who refused to submit to Orion's corporate wellness program.[132]

While these cases do not exactly mirror the privacy concerns articulated here, they may be instructive on the extent to which employees may protect health-related data collected from wearable sensors in the future.

3. The Electronic Communications Privacy Act

Another potential basis of legal protection is the Electronic Communications Privacy Act (ECPA), which makes it a crime to intercept or use electronic communications.[133] It is unlikely that the ECPA would limit employers' use of health data collected from employees.[134] One scholar, writing before health and fitness devices became common, concluded that the ECPA would not protect data contained in radio frequency identification (RFID) tags and read by RFID scanners.[135] He concluded that the transmitted data would not be an "electronic communication" within the scope of the ECPA.[136] Another obstacle to using the ECPA in this context is that it explicitly exempts "tracking devices," which it defines as "electronic or mechanical device[s] which permits the tracking of the movement of a person or object."[137] Because fitness devices like Fitbits and

130 Complaint, *EEOC v. Flambeau, Inc.*, No. 3:13-cv-00638 (W.D. Wis. Sept. 30, 2014).

131 Press Release, *EEOC Lawsuit Challenges Flambeau Over Wellness Program*, EEOC (Oct. 1, 2014), http://www.eeoc.gov/eeoc/newsroom/release/10-1-14b.cfm.

132 *EEOC v. Orion Energy Systems*, 1:14-cv-01019 (E.D. Wis. 2014); Press Release, *EEOC Lawsuit Challenges Orion Energy Wellness Program and Related Firing of Employee* (Aug. 20, 2014), http://www.eeoc.gov/eeoc/newsroom/release/8-20-14.cfm.

133 18 U.S.C. § 2511 (2012).

134 § 2511(2)(d) (allowing an exception if one party gives prior consent to such interception, such as through an employment contract).

135 Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Data?*, 22 SANTA CLARA COMPUTER & HIGH TECH L.J. 695 (2006).

136 *Id.* at 752.

137 *Id.* at 753 (citing 18 U.S.C. §§ 2510(12)(C), 3117(b) (2012)). When the term "tracking device" was defined in 1986, however, wearable health sensors as we know them

fitness apps installed on mobile phones are equipped with sensors, as most mobile phones are, they would likely qualify as "tracking devices," and therefore fall outside the scope of the ECPA.

4. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) might also limit wearable device monitoring at work.[138] Although no court has yet determined whether a wearable fitness sensor qualifies as a "computer" within the meaning of the CFAA, relevant precedent suggests that a court would do so.

Under the CFAA, a computer is:

> [A]n electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.[139]

When asked to determine whether a cell phone qualifies as a "computer" within the meaning of the CFAA, the Court of Appeals for the Eighth Circuit ruled that it did.[140] According to the Eighth Circuit, the CFAA's definition is "exceedingly broad" and "captures any device that makes use of a electronic data processor, examples of which are legion."[141] The rapid growth of technology, it noted, made it likely that more and more devices would qualify as computers for CFAA purposes over time. "As technology continues to develop," said the court, the CFAA's computer definition "may come to capture still additional devices that few industry experts, much less the Commission or Congress, could foresee."[142]

If employers access data from wearable devices or from the apps installed on their employees' mobile phones without employees' knowledge or consent, are they violating the CFAA? If the devices in question qualify as "computers" within the CFAA's "exceedingly broad" definition of that term, it would appear so. No court has yet addressed this specific question. Its resolution would likely

---

today were not widely used. *See* Pub. L. No. 99-508, § 108(a), 100 Stat. 1848, 1858 (1986) (codified as amended at 18 U.S.C. § 3117(b) (2012)).

138 Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

139 18 U.S.C. § 1030(e)(1) (2012).

140 United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011).

141 *Id.* at 903.

142 *Id.* at 903-04.

depend in part on whether the employer had engaged in fraud or abuse in connection with those devices or apps, which presumably would depend on the validity and extent of employee consent to the monitoring. The more commonplace such monitoring becomes, however, the harder it will be for employees to prove a lack of at least implied consent.

C. There Is No Effective Federal Agency Oversight of Employee Health and Fitness Data Collection

Several government agencies might play a role in protecting health and fitness data from employer misuse, including the FTC and the FDA.[143] This overlap of interests provides both an opportunity for interagency cooperation as well as a danger of redundant and inconsistent approaches to such regulation. As Professors Jim Rossi and Jody Freeman point out, shared regulatory space presents the challenge of coordination.[144] When more than one agency has authority to regulate an area, such coordination is necessary "to minimize inconsistency, maximize joint gains, plug gaps, and prevent systemic failures."[145] Professors Rossi and Freeman describe several forms of coordination, including consultation provisions, interagency agreements, joint policymaking, and centralized White House review.[146] In response, Eric Biber has pointed out the need for more empirical scholarship on the ways in which agencies interact with each other and with outside entities in order to make such coordination more effective.[147]

As discussed above, however, HIPAA, the most relevant regulatory framework overseen by HHS, may not extend to employers' use of health and fitness data collected from most mobile devices and apps, especially if an intermediary is used to collate and/or analyze the data. Judging from the explicit scope of its guidance, the FDA appears to be less concerned with the privacy

---

143 *See, e.g.*, Cora Han, Senior Attorney, Div. of Privacy & Identity Prot., Fed. Trade Comm'n, Remarks at the Internet of Things Workshop 165 (Nov. 19, 2013), http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf (introducing the Panel on Connected Health and Fitness).

144 Jim Rossi & Jody Freeman, *Agency Coordination in Shared Regulatory Space*, 125 HARV. L. REV. 1131, 1145 (2012).

145 *Id.* at 1149.

146 *Id.* at 1155.

147 Eric Biber, *The More the Merrier: Multiple Agencies and the Future of Administrative Law Scholarship*, 125 HARV. L. REV. F. 78 (2012) ("Research on [inter-agency operations] (whether by legal scholars or political scientists) will also require a lot more empirical research or understanding of how agencies function, and what motivates bureaucrats and political appointees.").

implications of mobile technology than its effectiveness in improving health.[148] The FTC is the most appropriate government agency to regulate the collection and use of employee health data, but serious questions remain about the effectiveness of its efforts in this area.

1. Food and Drug Administration Regulation

In January 2015, the FDA issued draft guidance on its plans to regulate certain "general wellness products," which may include fitness devices and software programs.[149] The FDA's guidance distinguishes between apps that effectively turn a mobile phone into a medical device and "general wellness products."[150]

Many of the health and fitness apps and devices that might transmit data of interest to employers fall into the FDA's "general wellness products" category. As illustrations of what might fall into this category, the FDA includes "a portable product that claims to monitor the pulse rate of users during exercise and hiking."[151] The Fitbit might be an example. The FDA classifies this as a "general wellness product" because "claim relates only to exercise and hiking and does not refer to a disease or medical condition" and because "the technology for monitoring poses a low risk to the user's safety." Other examples of "general wellness products" include "a mobile application that solely monitors and records daily energy expenditure and cardiovascular workout activities to "allow

148 *See, e.g., Mobile Medical Applications, Guidance for Industry and Food & Drug Administration Staff*, FOOD & DRUG ADMIN. 13 (2015), http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf ("FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended.").

149 *See General Wellness Policy for Low Risk Devices, Draft Guidance for Industry and Food & Drug Administration Staff*, FOOD & DRUG ADMIN. (2015), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429674.pdf. Covered devices "may include exercise equipment, audio recordings, video games, software programs and other products that are commonly, though not exclusively, available from retail establishments (including online retailers and distributors that offer software to be directly downloaded)." *Id.* at 2. One Washington-based law firm suggested that the FDA's draft guidance was motivated by the need to clarify the distinctions between more traditionally regulated medical devices and the fast-growing market of "general wellness products" that may be used for a range of health tracking purposes. *FDA Publishes Draft Guidance Describing General Wellness Claims*, COVINGTON & BURLING LLP (Jan. 26, 2015), https://www.cov.com/~/media/files/corporate/publications/2015/01/fda_publishes_draft_guidance_describing_general_wellness_claims.ashx.

150 *General Wellness Policy for Low Risk Devices*, *supra* note 149, at 2.

151 *Id.* at 7.

awareness of one's exercise activities to improve or maintain good cardiovascular health" and "a mobile application [that] monitors and records food consumption to manage dietary activity for weight management and alert the user, healthcare provider, or family member of unhealthy dietary activity."[152]

The FDA suggests that it has no plans to regulate these "general wellness products."[153] The device and both kinds of apps that appear as examples of these products could generate data that an employer might intercept, but those concerns are beyond the scope of the FDA's regulatory authority. Even if the FDA were to regulate these products, its primary concern would not be the potential for health and fitness data collection and sharing. The FDA's regulatory focus is the effectiveness and accuracy of these devices and apps rather than the privacy implications of their use.[154]

Professor Cortez has called for the FDA to become more engaged in the regulation of mobile health and fitness technology.[155] Indeed, two weeks after issuing its guidance on "general wellness devices," the FDA issued further guidance on "Mobile Medical Applications."[156] Recommendations included creating a new office for mobile medical technologies to educate consumers about apps that have health consequences for users and developing a requirement that app developers disclose the sources of medical information and calculations the app uses.[157] The FDA's more publications, however, suggest that the agency will not take any significant role in monitoring or restricting the use of employees' health and fitness data in the workplace.

2. Federal Trade Commission Regulation

The FTC also has the potential regulation of wearable health sensors in its sights. In January 2015, the FTC released a Staff Report called "Internet of Things: Privacy & Security in a Connected World." The report summarized findings that it had developed over the previous fourteen months, beginning with a workshop in November 2013. Privacy was a main topic of discussion

152 *Id.* at 6.

153 Thomas Sullivan, *FDA Device Guidance: General Wellness Policy for Low Risk Devices*, POL'Y &MED. (Jan. 29, 2015), http:// www.policymed.com/2015/01/fda-device-guidance-general-wellness-policy-for-low-risk-devices.html.

154 *See* Hall, *supra* note,109, at 32.

155 Cortez, *supra* note 62, at 1180-81(recommending that the FDA "confront its past regulatory failures and push itself into a regulatory 'feedback loop' in which the agency can identify past shortcomings and correct them going forward"); *see also* Nathaniel R. Carroll, *Mobile Medical App Regulation*, 7 ST. LOUIS U. J. HEALTH L. & POL'Y 415, 423 (2014). *But cf.* Thierer, *supra* note 3, at 71 (cautioning against overregulation of wearable technologies).

156 *See Mobile Medical Applications*, *supra* note 148.

157 *Id.*

throughout the workshop, as its title suggests, but participants' views were far from uniform. According to the Staff's subsequent report,

> Participants debated how the long-standing Fair Information Practice Principles ("FIPPs") of notice, choice, access, accuracy, data minimization, security, and accountability should apply to the IoT space. While some participants continued to support the application of all of the FIPPs others argued that data minimization, notice, and choice are less suitable for protecting consumer privacy in the IoT.[158]

In that workshop, the FTC devoted one of four panels to "Connected Health and Fitness," examining the "growth of increasingly connected medical devices and health and fitness products."[159]

In the January 2015 report, FTC staff acknowledged the danger that "unauthorized access to data collected by fitness and other devices that track consumers' location could endanger consumers' physical safety."[160] A greater risk, however, is the danger that employers could use data collected by those devices to make adverse decisions about and invade the privacy of its employees. Scott Peppet, a participant in the workshop and a professor at the University of Colorado Law School, noted the potential dangers of using such data to make employment decisions at the workshop, but FTC staff declined to adopt his larger concern.[161]

D. Device Makers and App Developers Provide Too Little Information to Protect Employees from Data Misuse

Can the health and fitness industry protect employee data well enough without regulatory intervention? Judging from the current state of the marketplace, I suspect not. The manufacturers of fitness devices that collect data currently face few restrictions on what data they can collect and how they can monetize it. Of course, sales from consumers provide one income stream, but downstream sales of data may be much more profitable. The potential profit from collecting, analyzing, repackaging, and selling health-related data to employers and/or marketers is barely limited by law. As it stands, app and device makers can now access a wide range of users' health-related data without those users' consent.

---

158 *Internet of Things: Privacy & Security in a Connected World*, FED. TRADE COMM'N 19 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

159 *Id.* at 3.

160 *Id.* at 13.

161 *Id.* at 16, 43-45. For a more expansive discussion of these concerns, see Peppet, *supra* note 3.

Scholars are beginning to ask important questions about the extent to which app developers and device manufacturers must disclose their data collection and sharing practices.[162] It can be hard for employees to find out how those personal health data are used or shared. Many health-related devices and apps lack clear indications of what they may be done with the data collected.

Technology providers pay at least lip service to protecting health-related data. In marketing its Health app, Apple reassures consumers that it takes their privacy concerns to heart:

> The information you generate about yourself is yours to use and share. You decide what information is placed in Health and which apps can access your data through the Health app. When your phone is locked with a passcode or Touch ID, all of your health and fitness data in the Health app is encrypted. You can back up data stored in the Health app to iCloud, where it is encrypted while in transit and at rest.[163]

There is a dichotomy, however, between industry assurances of consumer privacy and the rigors of the structures that would actually keep data private.

Apple encourages HealthKit developers to be transparent about their use of consumer data by asking them to "clearly disclose to the user how you and your app will use their HealthKit data."[164] This appears to be a suggestion rather than a contractual requirement. Apple itself distinguishes this and other "guidelines" from its "requirements" and urges HealthKit developers to make sure they comply with the latter.[165]

Apple does have contractual requirements regarding privacy that all app developers must follow, whether or not they use HealthKit.[166] According to

---

162 *See, e.g.*, Tobias Dehling et al., *Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Applications on iOS and Android*, 3 JMIR MHEALTH UHEALTH 1 (2015) (concluding that appropriate security measures need to be devised so that users can benefit from seamlessly accessible, tailored mobile health apps without potentially serious information security and privacy infringements); Anne Marie Helm & Daniel Georgatos, *Privacy and mHealth: How Mobile Health 'Apps' Fit into a Privacy Framework Not Limited to HIPAA*, 64 SYRACUSE L. REV. 131 (2014) (analyzing the privacy problems relevant to the different types of mobile health apps); Jennifer Bretts et al., Same Issues, New Devices: Is Smartphone App Privacy Groundhog Day for Regulators? (June 4, 2013) (unpublished manuscript), http://ssrn.com/abstract=2351189 (arguing that the lack of transparency and self-regulatory enforcement demonstrated by app permission exploitation shows the potential for continued circumvention of privacy regulation).

163 *Health: An Innovative New Way To Use Your Health and Fitness Information*, APPLE, https://www.apple.com/ios/whats-new/health (last visited Dec. 1, 2015).

164 *See The HealthKit Framework*, *supra* note 82.

165 *Id.*

166 *App Store Review Guidelines*, APPLE § 17 (2015), https://developer.apple.com/app-store/review/guidelines.

Apple, the only apps that require a privacy policy are those that "collect, transmit, or have the capability to share personal information . . . from a minor" and those that "include account registration or access a user's existing account."[167] HealthKit developers are subject to the additional requirement that they "must provide a privacy policy," but Apple does not mandate the content, appearance, or placement of such a policy.[168]

Apple also prohibits developers using the HealthKit framework from storing users' health information in iCloud and from using "data gathered from the HealthKit API for advertising or other use-based data mining purposes other than improving health, medical, and fitness management, or for the purpose of medical research."[169] Apple also notes that it will reject any app that "share[s] user data acquired via the HealthKit API with third parties without user consent."[170]

If an app developer were to violate these terms, however, it is not clear that the consumer whose data were sold would have a right of action against either Apple or the developer. Consumers may be incidental beneficiaries of these terms, but it is unlikely that a court would find that they had standing to sue either a developer for failing to follow them or Apple for failing to insist on them.

An alternative remedy could be to compel employers to disclose the extent to which they collect and use health data in employment decisions. It is hard to imagine how companies might be subjected to such a rule and how it might be enforced. As a further complication, it may be difficult to determine what impact, if any, health-related data may have on an employment decision ex post facto. Deciding what uses of health data are permissibly work-related may be especially challenging when the employer bears the cost of health insurance.

IV. TWO PROPOSALS WOULD RESTRICT EMPLOYERS' MISUSE OF HEALTH DATA

The lack of effective legal protection against the potential misuse of employee health data described in the preceding sections requires creative solutions. I propose two such solutions. One is designed to improve employee notice and decision-making about the disclosure of health and fitness data to employers by clarifying the terms and extent of such disclosure in advance. The other addresses the problem from the employer's end by limiting the potential collection and use of data.

167 *Id.* §§ 17.4, 17.5.
168 *Id.* § 27.7.
169 *Id.* § 27.4.
170 *Id.* § 27.5.

A. The FTC Should Require Standardized, Succinct Privacy Labels on Health and Fitness Apps and Devices

An important regulatory question is the extent to which app makers should be required to provide clear information about their privacy policies as a condition of use. One solution might be the implementation of a mandatory labeling regime for all apps and devices that collect health-related information. The labeling proposed here would provide all consumers, including the employees that are the focus of my concern in this article, with a more realistic and practical means of limiting access than they currently have.

1. Current Website Privacy Policy Requirements Suffer from Three Critical Deficiencies

A privacy labeling rule would correct many of the deficiencies from which current privacy policies suffer. While websites are currently required to have privacy notices, these notices are not an effective means of providing employees with meaningful choice about how their data would be shared. There are at least three problems with privacy policies as they currently appear on health and fitness-related websites.[171] First, it can be hard to locate them, especially on multi-page websites. Second, they are difficult and time-consuming to read. Third, they have inconsistent terms and scopes, making it hard to compare their practices.

One legal scholar has pointed out that a major problem with the privacy notices associated with health and fitness devices is that they are hard to find.[172] Professor Peppet describes his experience of opening a Breathometer device he had purchased, which measures blood alcohol content. The device came with a seventeen-page manual for using the device and opening the associated app, but the manual made no mention of a privacy policy. [173] Nor did the app itself when installed or the device upon startup. Nothing on the device, app, or manual disclosed whether the device collected any data other than blood alcohol content test results. In other words, it was not readily visible to the user. It did not disclose how any collected data might be stored, transferred, sold, or deleted. "Only by visiting the company's website, scrolling to the very bottom, and clicking the small link for 'Privacy Policy,'" Professor Peppet writes, "can one

171 Most wearable monitors, whether they are dedicated devices like a Fitbit or an integrated sensor in a smartphone, work in conjunction with apps rather than websites . Most products, however, also have related websites . Many app platforms, including Apple Health, require apps to post privacy notices . *See, e.g.*, *Privacy*, APPLE, https://www.apple.com/privacy/privacy-built-in (last visited Dec. 1, 2015).

172 *See* Peppet, *supra* note 3, at 89-90.

173 *Id.*.

learn that one's blood-alcohol test results are being stored indefinitely in the cloud, cannot be deleted by the user, may be disclosed in a court proceeding if necessary, and may be used to tailor advertisements at the company's discretion."[174] In sum, privacy policies associated with fitness devices may be so difficult to locate, requiring an effort that borders on research, that one might argue that they do not provide consumers with effective notice at all.

Not all health-related data collectors provide even this much information. Software manufacturer WelBe, whose products allow employers to aggregate employee health data from various sources, offers even less information about its privacy filters to the public. One has to scroll all the way to the bottom of the webpage to find a small link called "Privacy Policy."[175] Clicking on that link brings up the "O.C. Tanner Company Privacy Policy," which applies to all websites operated by what is apparently WelBe's parent company rather than to the WelBe products themselves.[176]

A second problem is that, even once they are found, it takes an unreasonably long time to read the notices. By one account, if someone were to read the privacy policy on every website she visits at least once a year, she would spend approximately 244 hours a year reading privacy policies.[177] Most privacy policies are cumbersome and difficult to interpret. The FTC itself has criticized the effectiveness of industry-generated privacy notices, observing that "the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[178] It is unrealistic to expect lengthy, obscure policy notices to provide the kind of meaningful choice that consumers want and that privacy legislation aims to provide.

Privacy policies may vary widely in substance even when such policies are required. Recognizing that consumers may have concerns about the privacy of their health data, Apple notes that "apps that access HealthKit are required to have a privacy policy," although it does not mandate the specific parameters of the policy.[179] In its instructions for developers, Apple refers them to two government websites for "guidance." One is a "Personal Health Record model

174 *Id.* at 90.

175 *See* WELBE, *supra* note 78.

176 *Company Privacy Policy*, O.C TANNER CO., https://www.awardselect.com/privacy/p_en_US.html (policy effective Sept. 19, 2013).

177 Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 540, 560 (2008).

178 *Protecting Consumer Privacy in an Era of Rapid Change*, FED. TRADE COMM'N iii (2010), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

179 *See The Healthkit Framework*, *supra* note 82.

(for non-HIPAA apps)," which links to the HealthKit's suggestions for a model privacy notice.[180] The other site is described as the "HIPAA model (for HIPAA covered apps)" and links to HHS privacy notice rules.[181] Apple does not, however, help developers determine whether their products are covered by HIPAA or not and consequently which set of guidelines they should follow.

2. Industry Self-Regulation of Privacy Policies Has Failed, Making Legislative Intervention Necessary

Consumer products sold in the United States are required to carry warranties that meet certain legibility requirements, pursuant to the Magnuson-Moss Warranty Act.[182] In passing that Act, Congress intended to make sure that consumers could get complete information about warranty terms and conditions, thereby helping them to make more informed purchases.[183] The Magnuson-Moss Warranty Act also allows consumers to compare warranty coverage among products before buying and promote competition on the basis of warranty coverage. By clarifying the sellers' obligations, the Act also makes it easier for consumers to pursue a remedy for breach of warranty in the courts.

One could argue that the same policy concerns underlie the need for clear data disclosure policies. Why should data disclosure policies be more difficult to interpret than warranties? The potential losses consumers could suffer as a result of the unauthorized use of their data—especially the health-related data that arguably would be protected under HIPAA if it were used by "covered entities"—could well exceed the potential financial losses that the Magnuson-Moss Warranty Act sought to limit.

The FTC appeared to be moving toward just such a labeling requirement. In 2012, FTC Chairman Jon Leibowitz announced, in 2012, plans to develop what the agency called a "Privacy Nutrition Label" for data collection and use.[184] As

---

180 *Id.*

181 *Id.*

182 Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975) (codified as amended at 15 U.S.C § 2301-12 (2012)).

183 S. REP. NO. 93-151, at 2 (1973) ("[T]his bill aims to increase the ability of the consumer to make more informed product choices and to enable him to economically pursue his own remedies when a supplier of a consumer product breaches a voluntarily assumed warranty or service contract obligation.");120 CONG. REC. 40711 (1974) (statement of Sen. Moss) ("By making warranties of consumer products clear and understandable through creating a uniform terminology of warranty coverage, consumers will for the first time have a clear and concise understanding of the terms of warranties of products they are considering purchasing.").

184 Josephine Liu, *FTC Working on Privacy "Nutrition Label"; Industry Focusing on Icons*, INSIDE PRIVACY (Oct. 25, 2012), http://www.insideprivacy.com/united-states/federal-trade-commission/ftc-working-on-privacy-nutrition-label-industry-focusing-on-icons.

envisioned at the time, this label would have contained "five essential terms" related to privacy although the FTC was still in the process of identifying those terms in conjunction with the Bureau of Consumer Protection. The FTC had considered adopting some form of standardized privacy labels, modeled after nutrition labels, as early as July 2001.[185] Since Leibowitz resigned from the FTC in 2013, however, there has been no further mention of government-mandated privacy labels for apps.[186]

The food labeling laws Congress has passed in recent years provide an apt analogy. The FDA enforces a complex series of food labeling laws that apply to all food products sold in the United States.[187] Beginning in the early twentieth century, certain furniture and bedding makers were required to label their products so that the public would know what materials were used inside (e.g., horse hair).[188] Labeling requirements have continued to evolve and extend in response to social changes. In late 2014, noting that Americans now "eat and drink about one-third of their calories away from home," the FDA announced new labeling rules that require certain restaurant chains to label menu items with nutritional information and all vending machines to provide calorie count labels for each item sold.[189] The rules extend nutrition label requirements in order to "help consumers make informed choices for themselves and their families."[190]

If the FDA can adapt labeling requirements to help consumers make more informed choices, it stands to reason that the FTC can develop privacy label requirements for health-related devices and apps for the same purpose. Although food consumption and data disclosure differ in some key ways, mandating the provision of more information about each can only help the consumer.

In its 2015 report on the IoT, the FTC agreed that "[w]hatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents."[191]

---

185 *Id.*

186 In June 2015, however, the FTC did propose to amend required privacy disclosures for motor vehicle dealers pursuant to the Gramm-Leach-Bliley Act, which would allow dealers to post these notices online. *See, e.g.*, 16 C.F.R. pt. 313 (2015).

187 *See, e.g.*, 21 C.F.R. § 101 (2015).

188 *See Law Label Learning Center*, AM. L. LABEL, http://www.americanlawlabel.com/law-label-learning-center/products (last visited Dec. 1, 2015).

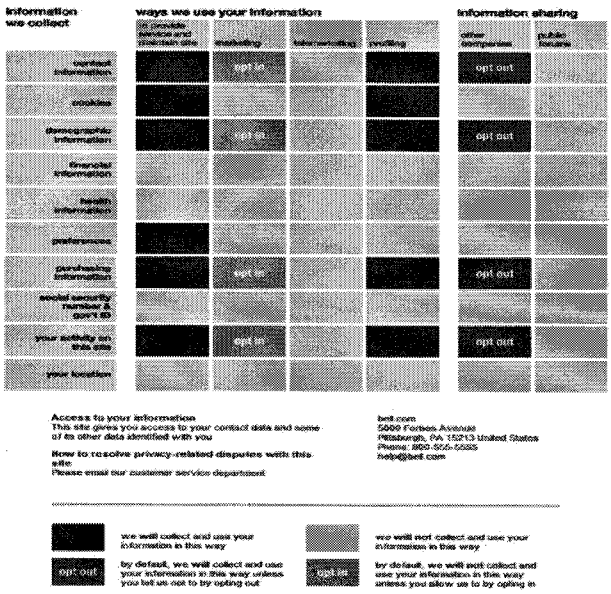
189 *See Menu and Vending Machines Labeling Requirements*, FOOD & DRUG ADMIN., http://www.fda.gov/Food/IngredientsPackagingLabeling/LabelingNutrition/ucm217762.htm (last visited Dec. 1, 2015).

190 *See Overview of FDA Labeling Requirements For Restaurants, Similar Retail Food Establishments and Vending Machines*, FOOD & DRUG ADMIN., http://www.fda.gov/Food/IngredientsPackagingLabeling/LabelingNutrition/ucm248732.htm (last visited Dec. 1, 2015).

191 *See Internet of Things*, *supra* note 161, at v.

There has been extensive research on the best formats for privacy nutrition labels already.[192] Researchers at Carnegie Mellon and other universities have developed privacy labels that indicate, at a glance, how a provider might use or share each of several kinds of information.[193] Here is a sample of such a label:

FIGURE: SAMPLE STANDARDIZED PRIVACY LABEL[194]



192 *See, e.g.*, Corey A. Ciocchetti, *The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices*, 20 JOHN MARSHALL J. COMPUTER & INFO. L. 1 (2008); Lorrie Cranor et al., *Spring Symposium: Data Privacy and Transparency in Private and Government Data Collection: Panel 1: Disclosure and Notice Practices in Private Data Collection*, 32 CARDOZO ARTS & ENT. L.J. 784 (2014); Daniel Parisi, *Mobile App Privacy: Developing Standard and Effective Privacy Tools for Consumers*, 15 N.C. J.L. & TECH. ONLINE ED. 240 (2014).

193 *See, e.g.*, *Privacy Nutrition Labels: Example Policy*, CYLAB USABLE PRIVACY & SECURITY LABORATORY, http://cups.cs.cmu.edu/privacyLabel; Patrick Gage Kelley et al., *A "Nutrition Label" for Privacy*, CYLAB USABLE PRIVACY & SECURITY LABORATORY (2009), http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf; *see also* KLEIMANN COMM'N GRP., INC., EVOLUTION OF A PROTOTYPE FINANCIAL PRIVACY NOTICE (Feb. 28, 2006), www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf.

194 *See Sample Privacy Label*, CYLAB USABLE PRIVACY & SECURITY LABORATORY, http://cups.cs.cmu.edu/privacylabel-05-2009/current/1.php (last visited Dec. 1, 2015). For a legend and more technical explanation of the figure, see *id.* Reprinted with the kind permission of Lorrie Cranor, Associate Professor, Computer Science and Engineering & Public Policy and Director, CyLab Usable Privacy and Security Laboratory at Carnegie Mellon University.

By providing standardized labels that are easy both to read and compare, providers would make it easier for consumers to make meaningful choices about the data they share. Apps and devices should be required to carry concise, effective privacy labels for this purpose. The privacy nutrition labels developed by the Cylab Usable Privacy and Security (CUPS) program at Carnegie Mellon University, led by Lorrie Faith Cranor, could provide an excellent starting point.[195]

While the CUPS model might serve as an initial framework, those in the legal community should consider two improvements. First, the standard data privacy label as it appears on websites should allow employees to click directly on the provisions to opt out of each kind of disclosure. The employees should receive an internet address along with the wearable that points them to an accompanying website. This site should describe the ways in which the data collected from the wearables should be used, abbreviated in the form of a label such as that shown above, and facilitate the opt-out process for each type of use. The labels' original architects envisioned this kind of opt-out provision but could not implement it when it was introduced due to a lack of standards for opt-out mechanisms.[196]

Second, a graphic version of this label should appear on the external packaging of all wearable fitness devices, just as nutrition labels must appear on the outside of packaged food sold in the United States. In a survey of twenty popular IoT consumer devices, not one of them included privacy indicia on the box.[197] The provision of an external, easy to read label, accessible to the consumer before the purchase, will help inform and improve purchasing decisions about products that can collect and share health data.

3. The Benefits of Mandatory Privacy Labels Will Outweigh the Costs

Professor Peppet suggests that regulators "seek industry consensus on best practices for where and when to give consumers notice about privacy and data issues."[198] He proposes a number of different measures that firms should commit to, including how to notify consumers about potential uses of their personal data, the location and capabilities of any sensors embedded within connected devices,

---

195 Other privacy label ideas have been proposed as well, such as Aza Raskin's development of a set of privacy icons at Mozilla . *See, e.g.*, Aza Raskin, *Privacy Icons: Alpha Release* (Dec. 27, 2010), www.azaraskin/blog/post/privacy-icons.

196 Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. TELECOMM & HIGH TECH L. 273, 289-90 (2012).

197 *See* Peppet, *supra* note 3, at 141. In fact, none of the surveyed devices made reference to a privacy policy on an associated website anywhere in the packaging materials or user guides. *Id.*

198 *Id.* at 163.

the data such sensors collect, and the length of time such data will be stored.[199] His recommendations, however, turn on the presumption that firms should be encouraged rather than required to adopt the policies he describes.[200]

I respectfully disagree with Professor Peppet's suggestion that firms can or should regulate themselves by developing standard policies. Other scholars have noted that industry is unlikely to develop more effective privacy notice and choice policies unless there is an incentive to do so.[201] The FTC itself has questioned the effectiveness of encouraging the industry collecting and using health data to self-regulate, noting in 2010 that "industry efforts to address privacy through self-regulation 'have been too slow, and up to now have failed to provide adequate and meaningful protection.'"[202] Lorrie Cranor notes that the state of privacy protections in 2012 closely resembled the state of such protections in 1996 when commentators first launched efforts to standardize website privacy practices.[203] According to Professor Cranor, "The experience over the past fifteen years demonstrates that privacy user empowerment tools and notice and choice mechanisms are insufficient to protect privacy . . . [E]nforcement mechanisms are needed to ensure that users' choices are respected."[204] Corey Ciocchetti has proposed such an enforcement mechanism in the form of federal legislation that would require collectors of personally identifiable information to provide "specific notice of intended third party recipients and their proposed uses prior to disclosure" as well as a private right of action.[205]

Suggesting new legislative remedies in scholarly articles is often seen as too cumbersome to be realistic. In this case, however, a legislative remedy may be the only realistic way to improve the protection of health-related data in the

---

199 *Id.* at 163-64.

200 *See id.* at 162-63 ("I would urge regulators and privacy advocates to encourage Internet of Things firms to adopt a simple principle: . . . These basic reforms to Internet of Things privacy policies are meant to begin a conversation between regulators, consumer advocates, privacy scholars, and corporate counsel. . . . [T]his conversation will take time and consensus building between regulators and market players.").

201 *See* Cranor, *supra* note 196, at 295; *see also* Cranor et al., *supra* note 192, at 788-89 (noting that incentive problems hampered the adoption of Platform for Privacy Preferences despite apparent industry consensus).

202 Press Release, Fed. Trade Comm'n, FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers.

203 *See* Cranor, *supra* note 196, at 275-76.

204 *Id.* at 304-05.

205 Ciocchetti, *supra* note 192, at 343; *see also* ROBERT SLOAN & RICHARD WARNER, UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND SECURITY 99-101 (2013) (discussing how informational norms could govern online business in greater detail) .

employment context. Voluntary programs to develop data privacy disclosures have done little to improve consumer or employee protection. Recommendations that rely on industry to make it easier for consumers to limit the data that industry potentially can sell have, perhaps unsurprisingly, failed repeatedly over the last two decades. As Lauren Henry Scholz observed:

> The data-gathering company has an incentive to conceal or deemphasize its personal information collection practices, which otherwise may discourage consumers from providing personal data. Typically, consumers cannot differentiate between a product or business practice that has strong data security and privacy provisions from one lacking such provisions. Consumers who desire greater privacy protections thus will be unable to select and pay more for a product that is better in that respect. Therefore, market actors do not have an incentive to provide such products.[206]

Another benefit of legislation is the corresponding enforcement power. Enforcement presumably would address not only the provision of privacy labels but their accuracy as well. There is reason to suspect that app developers and website providers might misrepresent their practices absent such enforcement. Scholars found that websites voluntarily posting privacy policies in order to comply with an earlier web standard, Platform for Privacy Preferences, frequently misrepresented their privacy policies in order to get more favorable placement within the web browser Internet Explorer.[207] While consumers could also sue providers for fraud, the potential costs of doing so and problems of quantifying injury from invasions of privacy may deter that kind of litigation.[208] Developing a labeling requirement like this will pose challenges. None of these challenges outweigh the significant benefits that a privacy labeling program would provide.

One problem in implementing this type of privacy label program is that there is already a competing—although not mandatory—privacy labeling regime. The Office of the National Coordinator for Health Information Technology has

---

206 Lauren Henry Scholz, *Institutionally Appropriate Approaches to Privacy: Striking a Balance between Judicial and Administrative Enforcement of Privacy Law*, 51 HARV. J. ON LEGIS. 193, 195 (2014).

207 Pedro Giovanni et al., *Token Attempt: The Misrepresentation of Website Privacy Policies Through the Misuse of P3P Compact Policy Tokens*, CYLAB (2010), www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab10014.pdf.

208 In December 2011, a judge dismissed a class action against Amazon for misrepresenting privacy policies because the plaintiffs failed to allege the minimum financial harm required with sufficient specificity. *See* Order Granting Defendant's Motion to Dismiss, Del Vecchio v. Amazon.com, Inc., No. C11-366-RSL (W.D. Wash. June 1, 2012); Venkat Balasubramani, *The Cookie Crumbles for Amazon Privacy Plaintiffs*, TECH. & MARKETING L. BLOG (Dec. 2, 2011), http://blog.ericgoldman.org/archives/2011/12/the_cookie_crum.htm.

established a Personal Health Record (PHR) Model Privacy Notice. Its goal is to provide a template that a "web-based PHR company can use to succinctly inform consumers about its privacy and security policies."[209] By its terms, the PHR Model Privacy Notice is not required of companies that collect health data online, although it was apparently inspired by mandatory labeling regimes.[210] Like the CUPS label, the PHR Model Privacy Notice "is meant to be similar to other consumer-oriented 'labels' that have been developed for other industries, such as the nutrition facts label for food and the Model Privacy Notice developed for the financial services industry for compliance with the Gramm-Leach-Bliley Act."[211]

A second challenge of such a regime is that the additional labeling may add cost, which ultimately will be passed on to the purchaser. The cost of changing product packaging to include standardized packaging labels is likely to be minimal, however, especially relative to the cost of consumer electronics. Since every product will bear the same cost, no provider will be at a competitive advantage or disadvantage vis-à-vis these costs. Finally, research has shown that consumers are willing to pay a bit more to buy goods from more secure sites when they were given information about how the sites shared their data.[212]

Reaching consensus on a privacy labeling regime may be difficult. Several federal agencies are likely to play some role in developing such a regime, which therefore will require inter-agency collaboration. There is precedent, however, for multiple government agencies working together to develop a comparable labeling requirement. Eight government entities collaborated and jointly announced the final Model Privacy Notice required by the Gramm-Leach-Bliley Act. The Act requires financial organizations to send this notice to their customers.[213] The eight entities were required to work jointly on the model notice

---

209 *Personal Health Record (PHR) Model Privacy Notice*, HEALTH IT, http://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-model-privacy-notice (last visited Dec. 1, 2015).

210 Office of the Nat'l Coordinator for Health Info. Tech., *About the PHR Model Privacy Notice: Background, Development Process and Key Points*, HEALTH IT 2 (2011), http://www.healthit.gov/sites/default/files/phr-model-privacy-notice-backgrounder-final.pdf ("Like the FDA nutrition facts label, the Model Notice is intended to enable companies to present complex information in a manner that is accessible, consistent, and conducive to informed choice. Unlike the FDA nutrition facts label, use of the Model Notice is voluntary.").

211 *Id.*

212 *See* Cranor, *supra* note 196, at 292-93.

213 These were the Federal Reserve Board, the Office of Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, the Federal Trade Commission, the Securities and Exchange Commission, and the Commodity Futures Trading Commission. *See* 79 Fed. Reg. 64,057 (Oct. 28, 2014) (to be codified at 12 C.F.R. pt. 300).

by Section 728 of the Financial Services Regulatory Relief Act of 2006.[214]

If those entities can work together to develop a model notice (which took the form of a table), then there is reason to believe that the FTC, the Federal Communications Commission (FCC), the FDA, and other interested agencies should reasonably be able to cooperate on a model health data privacy label. The FTC's leadership on this issue may also facilitate interagency cooperation. While other agencies have an interest in the development of privacy labels and should be consulted, the FTC has the clearest mandate both to lead the regulation and to enforce it.

A final shortcoming of this solution is that it does little to address the concerns of employees who are required to wear health and fitness sensors, and therefore have limited choice in the devices they use. If employers choose the devices for their employees, through corporate programs like Fitbit Wellness or Jawbone's UP for Groups, such a privacy regime may be even less protective. Improving the information available to employees about the monitoring systems used, however, will make these practices more transparent.

B. Extend HIPAA's Definition of Covered Entities to Include Employers, App Developers and Wearable Device Manufacturers

My second recommendation would restrict employers' use of health and fitness data more than federal laws currently do. While I believe that a legislative solution is necessary for reasons described below, this Article does not propose entirely new legislation to curtail the use of these data. A regulatory structure is already in place for the protection of health-related data in the form of HIPAA. As discussed above, the current definition of "covered entities" under HIPAA excludes device manufacturers and app developers. Including these entities in a revised definition of "covered entities" would extend protection against the misuse of employees' health-related data. Similarly, expanding the definition of "[i]ndividually identifiable health information" to data generated by mobile health and fitness sensors, including those built into mobile phones and smart watches as well as dedicated fitness devices, would bring more of these data within the scope of HIPAA protection.

Much of the administrative detail that would be needed to protect employee health and fitness data also exists in HIPAA. The Security Rule, for example, specifies steps that covered entities must take to ensure the confidentiality and integrity of electronic personal health information.[215] It also protects against the

214 Financial Services Regulatory Relief Act of 2006, Pub. L. No. 109-351, 120 Stat. 1966.

215 HIPAA Security Rule, 45 C.F.R. pts. 160, 164(A), 164(C) (2003).

uses and disclosure of such information.[216] In fact, the HIPAA Security Rule is one of the most detailed and prescriptive of all U.S. information security laws.[217] The Health Information Technology for Economic and Clinical Health (HITECH) rules that amend existing HIPAA obligations provide sufficient coverage to extend the protection of data to entities that work with employers, for example, by collecting or interpreting employee health data for those employers. Under the HITECH rules, such entities may be considered Business Associates and therefore be subject to certain restrictions on the use and transfer of personal data.[218]

Finally, Congress should amend HIPAA to provide a private right of action. As one scholar has pointed out, such a provision would be similar to, and no less justified than, the private right of action Congress included in the Fair Credit Reporting Act for negligent disclosures by credit agencies.[219]

C. Securing Employee Health Data Requires Additional Study and Discussion

Neither of the two solutions proposed here is sufficient—alone or taken together—to completely protect personal health-related data from potential employer misuse. These suggestions will not resolve all of the legal and ethical problems concerning employers' acquisition of employees' health and fitness data described in this Article. For example, if the FTC were to require privacy nutrition labels like the ones suggested here, there presumably would be no private right of action. Employees whose health and fitness data were shared in a manner inconsistent with the privacy product labeling could not seek redress directly from the manufacturer or developer, but would instead have to rely on the FTC to enforce its directives. Since the FTC retains enforcement discretion, an employee may not have a remedy against the manufacturer or employer. In addition, neither solution resolves the underlying problem of potential vagueness as to what constitutes protectable information.

The legality of health data privacy at work should also be part of a larger discussion about the modern value of privacy in general. As Kate Murphy wrote in a widely shared *New York Times* essay, people both value privacy and cannot

---

216 HIPAA Privacy Rule, 45 C.F.R. pts. 160, 164(A), 164(E) (2003).

217 *Getting the Deal Through: Data Protection and Privacy in 26 Jurisdictions Worldwide 2014*, HUNTON & WILLIAMS LLP (2014), http://www.hunton.com/files/Publication/1f767bed-fe08-42bf-94e0-0bd03bf8b74b/Presentation/PublicationAttachment/b167028d-1065-4899-87a9-125700da0133/United_States_GTDT_Data_Protection_and_Privacy_2014.pdf.

218 78 Fed. Reg. 5566 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160 & 164).

219 Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1114 (1971) (codified as amended in scattered sections of 12 and 15 U.S.C. (2012)); Zivanovic, *supra* note 3, at 199.

seem to stop sharing information.[220] As Murphy noted, a three-year German study showed a privacy paradox in that the more people disclose about themselves, at least on social media, the more privacy they desire.[221] While there may be a benefit to measuring the biometric data of workers, employers risk sacrificing the quality of their work. According to Murphy,

> Privacy research in both online and offline environments has shown that just the perception, let alone the reality, of being watched results in feelings of low self-esteem, depression and anxiety. Whether observed by a supervisor at work or Facebook friends, people are inclined to conform and demonstrate less individuality and creativity. Their performance of tasks suffers and they have elevated pulse rates and levels of stress hormones.[222]

These studies have another implication that employers should value. They suggest that performance suffers when employees experience a loss of privacy. Of course, employers need to monitor their employees to a certain extent as they have always done. What this research suggests, however, is that an increase in biometric and health data collection may correlate with a decrease in work performance quality.

CONCLUSION

Health data collected from wearable technology may affect employment decisions and status in ways that U.S. law has never before permitted. Business analysts predict that the amount of employee-generated health and fitness data will rise exponentially over the next several years. At the same time, employers' ability to collect, analyze and act on these data are essentially unfettered by law. Employers have every incentive to use these data for a variety of purposes. Many of them are finding new ways to do so now, aided by insurers and data providers. Employees have little legal protection from employment practices that hinge on access to their health and fitness data. While the use of these data may be risky for the monitored employees, there may be no federal basis of liability for employers for any consequent harm. Employees therefore face a growing risk, with no clear legal remedy.

While the legal risks associated with employer use and collection of employee health and fitness data are starting to attract scholarly attention, better solutions are needed. In this Article, I have proposed two specific solutions that

220 *See* Murphy, *supra* note 96.

221 PRIVACY ONLINE: PERSPECTIVES ON PRIVACY AND SELF-DISCLOSURE IN THE SOCIAL WEB (Sabine Trepte & Leonard Reinecke, eds. 2011), http://www.springer.com/computer/general+issues/book/978-3-642-21520-9.

222 Murphy, *supra* note 96.

would offer monitored employees more notice, choice and remedy regarding these practices. A mandatory privacy labeling law for fitness devices and health-related apps would help employees to better understand the health data that employers can access from their use. Extending the terms of HIPAA to cover employers as well as medical professionals and health and fitness data generated from popular mobile sensors as well as more traditional medical records, would align expectations of health privacy with a legal right to that privacy. While neither solution is perfect, they provide a basis for further discussion of the best ways to address this growing problem.